HITACHI
Inspire the Next

情報セキュリティ報告書 2020

Information Security Report 2020

INDEX

〈本報告書の概要〉

●報告範囲・期間：2019年度までの日立グループにおける情報セキュリティの取り組み

●報告書の発行時期：2020年12月発行

加速する事業変革やグローバル経営下で情報セキュリティのさらなる強化を

— 昨今のITを取り巻く環境の変化が事業に及ぼす影響について、CISO（最高情報セキュリティ責任者）の視点から考えをお聞かせください。

情報のクラウド化やデジタル化は進んでいますし、今までのレガシーな情報セキュリティのやり方をさらに進歩させていかなければ、立ち行かなくなっていきます。新型コロナウイルス感染症の拡大を契機としてリモートワークが急速に浸透し、環境の整備も加速度的に進んでいます。その一方で、情報セキュリティに対する脅威はかつてない別次元の領域に突入しつつあり、さまざまな環境下で働く人たちを最新のセキュリティでプロテクトしていくことが必要です。

— 個々人のセキュリティリスクに加え、多角化が進む事業におけるリスクはどうでしょうか。

M&Aやカーブアウトなどの経営戦略を推進するうえで、市場での競争力を高めるためのシステム統合が、思わぬセキュリティリスクを誘発する危険性をはらんでいます。新たに加わっていただく企業には従来のセキュリティ基準があるわけですが、日立グループのものとダブルスタンダードにしておくわけにはいきません。移行期間を設けて速やかに統合監視するなどの対策が必要です。一方カーブアウトの場合は先方のセキュリティ管理下に入るまで、我々がしっかりと責任を持つ必要があります。グローバルレベルの経営戦略となると、リスクのポテンシャルは国を越えて広がっていきますが、やるべきことは同じです。

— 日本でも複数の企業がサイバー攻撃を受けています。この動向をどう捉えますか。

サイバー攻撃はどの企業でも起こりうることですし、現在では企業のみならず、国際社会を脅かすレベルにまで達しています。もはや、これまでのように高い壁をつくって侵入を防ぐという考え方だけでは対処できません。常に進化しているサイバー攻撃に対して、「リスクは入ってくるものだ」ということを前提とした防御策を講じる段階を迎えています。

— これからの防御策としてどのようなことが考えられますか。

当然最新のテクノロジーを活用した環境を構築していくことが必要です。さまざまな弱点を突いてこられる可能性がありますので、それらを食い止めるだけでなく、万が一入ってこられたとしても速やかに対処できる仕組みを作っておくことが大切です。いかに早く見つけ、いかに最小限に食い止めるか、です。その際ポイントとなるのはセキュリティの多様性です。画一的な基準やマニュアルに任せきりになると突破された場合、被害が拡大する恐れがあります。多様な対策を講じておくことが大切で、例えばヨーグルトのフタのようなセキュリティの考え方も必要です。

— ヨーグルトのフタ！　それはどういう発想のセキュリティなのでしょうか。

ヨーグルトがランサムウェアでヨーグルトのフタがセキュリティシステムだと置き換えてみてください。近頃、フタの内側には凹凸が加工されていて、付着したヨーグルトが簡単に流れ落ちるようにできています。いわば、この発想がサイバー攻撃に対する考え方にも当てはまります。対策を同じにするのではなく、あえて多様性を持たせることで、リスクの侵入を防ぐのです。リスクから逃げるのはなくリスクと対峙（たいじ）するのです。

— セキュリティ自体も変わりつつあることを感じます。鍵を握るのは何でしょうか。

やはり、人でしょうか。最新の動向を常に把握し、傾向分析して、すばやく情報連携できる人財を社内で育成していきたいと考えます。セキュリティはネガティブなイメージがあるかもしれませんが、さまざまな手法で仕掛けてくるサイバー攻撃を撃退するミッションに誇りと喜びを感じながら、積極的に事業活動を支援できる人財を増やしていく予定です。

— 今後の日立グループとしての方向性をお聞かせください。

日々進化する脅威に対して一社でできることには限界があります。国内外のグループ会社はもちろん、社外パートナーと緊密な連携を取り、サイバー攻撃の情報を共有しながら大きな面で防御していくことも必要です。そのような対策を講じることにより日立グループとして情報セキュリティ事故を未然に防ぐとともに、万が一に備え、事業に及ぼす影響を最小限に食い止める努力と工夫を日々続けていきます。グローバルな企業活動が活発化していく今後、情報セキュリティの領域において、諸活動を通して日立グループのプレゼンスを高めていきたいと考えています。

株式会社日立製作所
執行役常務　CTrO兼CISO
村山 昌史

1985年入社。Smart Transformation Project強化本部プロジェクト・マネジメント推進室長といった経験を生かし2016年からCPO兼バリューチェーン・インテグレーション統括本部長として調達関係の戦略策定や、構造改革をけん引。2019年執行役常務、2020年CISO就任。

情報セキュリティガバナンス

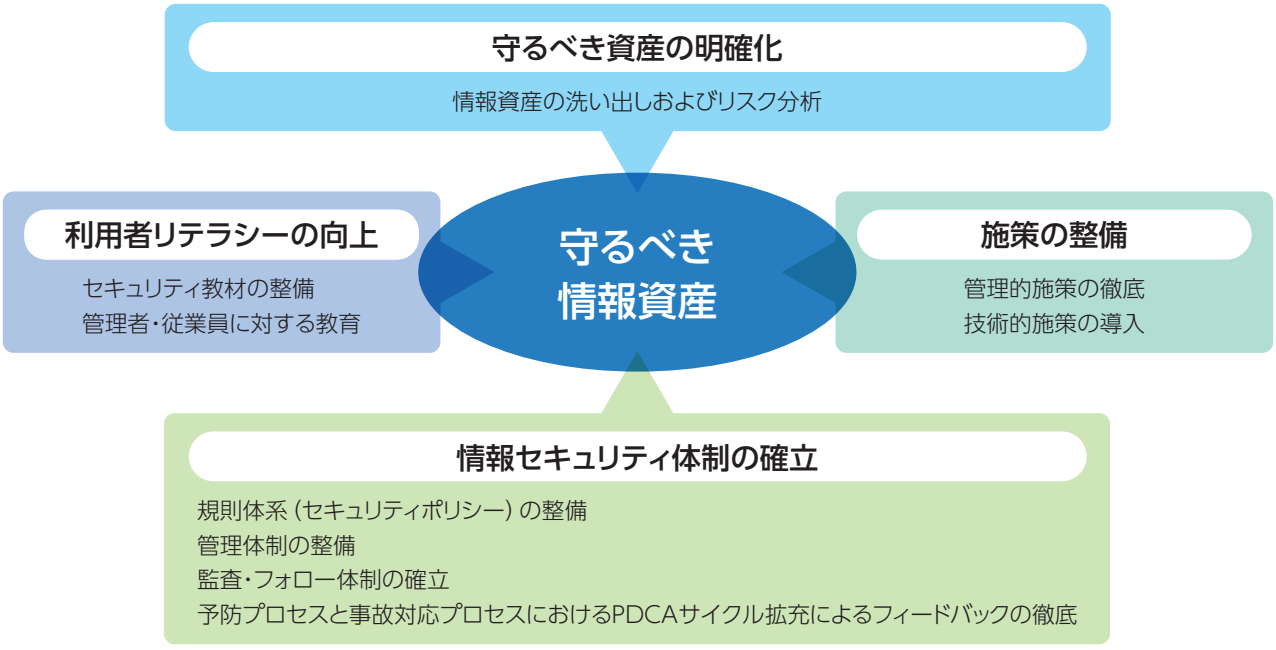
情報セキュリティガバナンスの基本的な考え方

IoTの進展により、さまざまなモノがつながることで、新たな価値が生み出されています。その一方で、日々巧妙化するサイバー攻撃の対象も従来のITからモノのインターネットといわれるIoTや、制御・運用技術であるOTの分野にまで広がっています。情報漏えいや操業停止など、事業そのものの継続に支障をきたすリスクを最小化するため、情報セキュリティにかかわるリスクマネジメントは、企業の最重要の課題の一つとなっています。

こうした背景のもと、社会イノベーション事業のグローバルリーダーをめざす日立は、価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることを重要な経営課題の一つと位置付け、情報セキュリティのガバナンスに取り組んでいます。

情報セキュリティの取り組み

お客さまからお預かりした情報やそれを保管するシステム、また社会インフラのサービスを行う情報システムなどさまざまな守るべき情報資産を保護するために、事故は「必ず起こるもの」という前提に立ち、4つの観点で情報セキュリティに取り組んでいます。また、日立製作所主導により、日立グループの情報セキュリティマネジメントシステムのPDCAサイクル（継続的改善活動）を推進し、世界各国の日立グループでセキュリティレベルの向上に取り組んでいます。



情報セキュリティマネジメント

日立の情報セキュリティに関する方針、推進体制、規則、マネジメントサイクルなどの概要について紹介します。

情報セキュリティの方針

日立は、日本を代表するグローバル企業として、セキュリティリスクを経営リスクの一つとして認識し、企業の経営方針を織り込んだセキュリティの方針を定め、情報セキュリティの確保に努めています。

(1) 情報セキュリティ管理規則の策定および継続的改善

当社は、情報セキュリティの取り組みを、経営ならびに事業における重要課題のひとつと認識し、法令およびそのほかの規範に準拠・適合した情報セキュリティ管理規則を策定する。さらに、当社役員を中心とした全社における情報セキュリティ管理体制を確立し、これを着実に実施する。加えて組織的、人的、物理的および技術的な情報セキュリティを維持し、継続的に改善していく。

(2) 情報資産の保護と継続的管理

当社は、当社の扱う情報資産の機密性、完全性および可用性に対する脅威から情報資産を適切に保護するため、安全な管理策を講じる。また、事業継続のために、適切な管理措置を講じる。

(3) 法令・規範の順守

当社は、情報セキュリティに関する法令およびそのほかの規範を順守する。また、当社の情報セキュリティ管理規則を、これらの法令およびそのほかの規範に適合させる。また、これらに違反した場合には、社員就業規則などに照らして、しかるべき処分を行う。

(4) 教育・訓練

当社は、当社役員および従業員へ情報セキュリティの意識向上を図るとともに、情報セキュリティに関する教育・訓練を行う。

(5) 事故発生予防と発生時の対応

当社は、情報セキュリティ事故の防止に努めるとともに、万一、事故が発生した場合には、再発防止策を含む適切な対策を速やかに講じる。

(6) 企業集団における業務の適正化確保

当社は、前第1項から第5項に従い、当社および当社グループ会社からなる企業集団における業務の適正を確保するための体制の構築に努める。

情報セキュリティ推進体制

日立グループにおいては、日立製作所 本社（コーポレート）がグループ全体のガバナンスを行います。

日立製作所の各ビジネスユニット（以下、BUと記す）・事業所およびグループ会社に対して各統制ラインより実行の指示を行うことでガバナンスを実現します。また、BU・グループ会社はそれぞれのグループ会社（子会社）に対しても同様の統制を行うことでグループ経営を実現しています。これは日本国内だけではなく海外に対しても同様となります。

執行役社長が、情報セキュリティについて責任と権限を有する情報セキュリティ統括責任者と、情報セキュリティ監査について責任と権限を有する情報セキュリティ監査責任者を任命します。

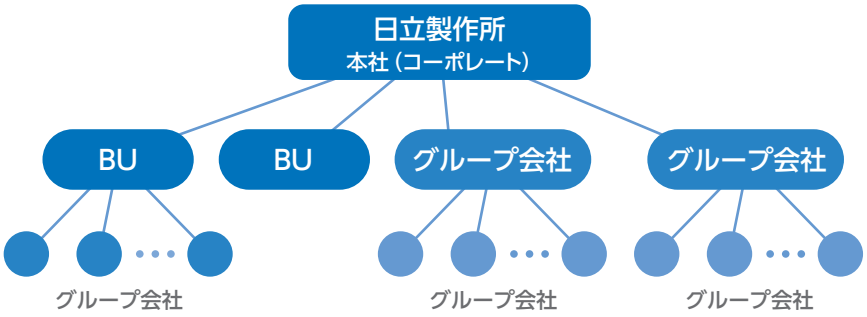
情報セキュリティ統括責任者は、情報セキュリティ委員会を組織し、情報セキュリティに関する方針、個人情報保護方針、教育計画、各種施策を決定します。

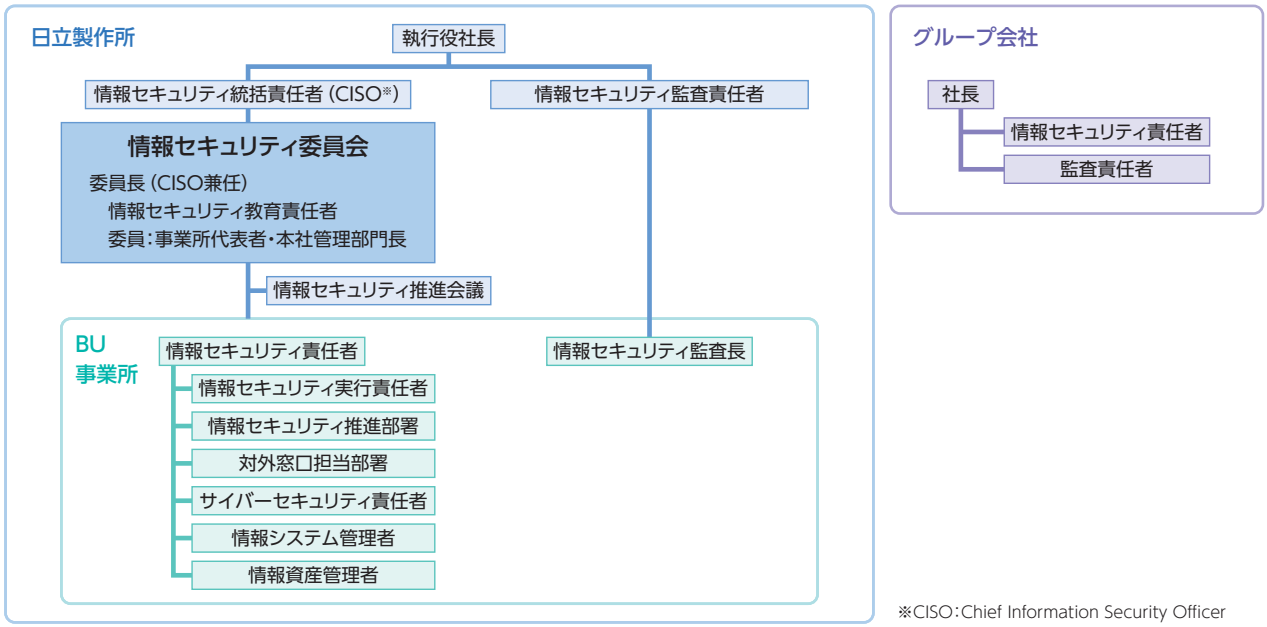
情報セキュリティ委員会の決定事項は、全BU・事業所実務者が出席する情報セキュリティ推進会議を通じて、各組織に徹底されます。

BU・事業所では、原則BU長・事業所長が情報セキュリティ責任者を務めます。

また情報セキュリティ推進部署を設置し、各組織の個人情報保護、情報セキュリティ、機密情報管理、入退管理、外注管理に対応するとともに、従業員に対して教育を行います。また各部署には情報資産管理者を置き、個人情報を含む情報資産の取り扱いに関する責任体制を整えています。

グループ会社においても同様の組織を設け、互いに連携して横断的な情報セキュリティを推進しています。





※CISO：Chief Information Security Officer

情報セキュリティ規則体系

情報セキュリティの方針に基づき、下表の規則を定めています。
また、グループ会社も同等の規則を定め、情報セキュリティを推進しています。

分　類	規則名
基本規則	情報セキュリティマネジメント総則
	情報及び情報機器の取扱い総則
	機密情報管理規則
	個人情報管理規則
個別規則	Webサイト及び情報開示に関する規則
	情報セキュリティシステム管理規則
	入退及び立ち入り制限区域管理規則
	個人情報取扱業務委託規準

●基本規則

「情報セキュリティマネジメント総則」は、情報セキュリティマネジメントシステムの策定、実施、維持、継続的な改善に関する基本的な順守事項を定めています。「情報及び情報機器の取扱い総則」は、情報全般の漏えい、情報の不正利用による事故を防止することを目的に、情報および情報機器の取り扱いと管理に関する基本的な事項を定めています。

「機密情報管理規則」は、機密情報の保全に関する取り扱いを定めています。

●個別規則

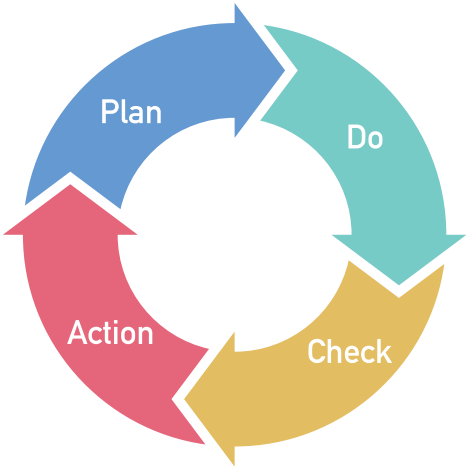
「Webサイト及び情報開示に関する規則」は、Webサイトにおいて、情報の開示および利用を正しく行うために順守すべき事項を定めています。

「情報セキュリティシステム管理規則」は、情報システムにおいてセキュリティを確保する手段について定めています。

「入退及び立ち入り制限区域管理規則」は、建物への入退管理に関する規定など、物理的なセキュリティの確保について定めています。

情報セキュリティマネジメントサイクル

個人情報マネジメントを含む情報セキュリティマネジメント全体をPDCA (Plan-Do-Check-Action) として実施するフレームワークを構築し、[Plan]ルール・施策を定め、[Do]施策を実施し、[Check]啓発・モニタリングを行い、[Action]継続的改善を通じて、半年サイクルで実行します。



情報セキュリティに関する教育

●情報セキュリティ教育

情報セキュリティを守り、個人情報や機密情報を保護するためには、従業員一人ひとりがその重要性を理解し、日々の業務の中で意識して行動する事が必要です。

日立では、すべての役員、従業員、派遣社員などを対象に、情報セキュリティ・個人情報保護についてeラーニングによる教育を毎年実施しています。日立製作所では従業員など約4万人が受講し、受講率は100%に達しています。そのほかにも、毎年情報セキュリティ教育計画を策定し、新入社員、新任管理職といった階層別教育や個人情報保護担当者などを対象とした専門教育など、対象別、目的別に多様な教育プログラムを用意して実施しています。

日立製作所の教育コンテンツは国内外のグループ会社にも公開しており、日立グループ全体として情報セキュリティ・個人情報保護教育に積極的に取り組んでいます。

分　類	対象者	内　容
全従業員教育	・全従業員 ・派遣社員 ・出向受入者	個人情報保護および機密情報管理の必要性、情報セキュリティ最新情報
階層別教育	経営幹部	個人情報保護の動向と日立製作所の取り組み
	課長相当職	個人情報保護、機密情報管理、情報セキュリティについて管理職として必要な知識および日立製作所の個人情報保護の取り組み
	新入社員	個人情報保護、機密情報管理、情報セキュリティに関する基本的な知識
専門教育	個人情報保護担当者	個人情報保護担当者個人情報保護担当者として必要となる、社内規則体系や管理体系、実運用手順などの専門的な知識および事例を踏まえた実践演習
	情報資産管理者	各部署で個人情報を含む情報資産の管理責任者として行動するために必要な知識

情報システムや情報セキュリティに携わるより専門的な教育については「セキュリティ人財育成の取り組み」に記載しています。

●標的型攻撃メール訓練教育

標的型攻撃メールによるサイバー攻撃は日々行われており、従業員が攻撃を受けた場合、適切に対応できるよう一人ひとりの訓練が欠かせません。

日立では2012年よりグループ会社も含めて全従業員を対象とした標的型攻撃メール訓練教育を実施しています。実際に標的型攻撃メールを装った模擬メールを各人に送付して、不審メールとはどういうものか、受信した際にどのように対応すべきかなどについて、実体験を通して対応力の強化を図っています。

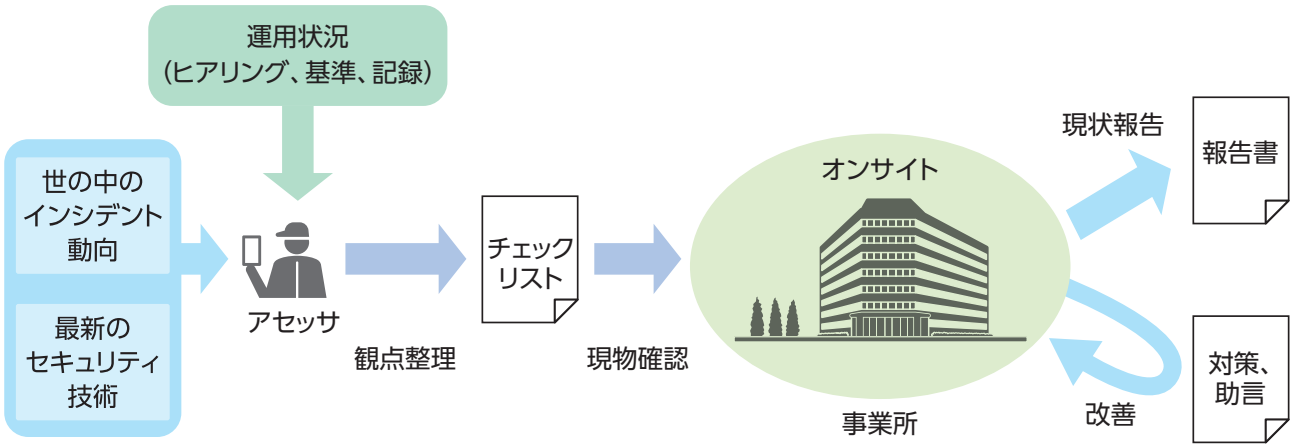
オンサイトセキュリティリスクアセスメント

グローバルに事業を展開する日立グループでは、各国・各地域に多くの拠点を構えており、本社機能、営業所、サービスや製造拠点などさまざまな事業形態があります。このような環境下において組織内のネットワークの環境や設備、IT機器などの設置や利用環境も多様である一方で、インターネット接続やリムーバブルメディア(USBメモリ)などを経由した社外とのコミュニケーションを行うため、標的型攻撃やマルウェア感染などのセキュリティリスクへの備えが重要となってきます。

事業を取り巻く環境の変化に伴うリスクに対応するために、セキュリティ専門家チームによるアセスメント体制を強化しています。具体的にはBU・グループ会社の現場を訪問し、次の視点から強化施策に取り組んでいます。

① 日立グループのネットワークにつながるすべての製品や社内設備を対象に、セキュリティ専門家チームが最新動向を踏まえたアセスメントを行う

② セキュリティ上のリスクとなる課題の抽出と解決に向け現場に対し有効な対策の提言



2019年度は19社の国内・海外拠点の現場のアセスメントを行い、セキュリティリスクを多数摘出し、必要な対策についてアドバイスしています。また、全社的な問題については施策にフィードバックを行っています。

2020年度は新型コロナウイルスの影響で現場確認ができないため、リモート確認などさまざまな代替手段を用いたアセスメントを計画しています。

コラム

新しい日常を支えるサイバーレジリエンス強化に向けて

昨今の企業を取り巻くサイバーセキュリティは多くの課題に直面しています。サイバー攻撃の手口は以前に増して高度化し、攻撃の量も増加し、攻撃対象の範囲も拡大の一途をたどっています。また、新潮流であるデジタルトランスフォーメーションへの追従や、コロナ渦によって急速に進展した新しい働き方への対応など、効率的かつ安全に業務を遂行するためのセキュリティ対策を迫られている状況です。

日立は、あらゆる事業活動の維持・拡大のため、組織の垣根を越えてセキュリティという1つの目標に向け連携する「セキュリティエコシステムの構築」に取り組んでいます。そして、従業員一人ひとりが自発的にセキュリティに取り組む意識を醸成する「新たなセキュリティ啓発活動」をスタートさせます。

1 セキュリティエコシステムの構築　3つの「つながる」によるセキュリティの信頼性向上

(1) モノが「つながる」

デジタルトランスフォーメーションでは、さまざまなつながりが新たな付加価値の創出や社会課題の解決をもたらします。これらを実現するために、IoTに代表される機器やシステムなどのモノが「つながる」環境になります。

これに対し、日立では、あらゆる環境において網羅的なサイバーセキュリティ対策に取り組んでいます。

(2) 人・組織が「つながる」

いままでつながっていなかったモノが「つながる」中でセキュリティを確保するには、異なる組織が相互に協力して対策を推進することが必要になります。

統制による対策徹底に加えて、立場、組織の垣根を越えたコミュニティづくりを行い、自身の役割を再認識すると同時に、周囲との連携を深めることで、人・組織が「つながる」活動を推進しています。

(3) 社会が「つながる」

また、つながりは日立の中だけに限ったことではありません。サイバーセキュリティ対策に取り組んでいる国、学校、企業との脅威情報や対策実行時の課題共有など、枠組みを越えたコミュニティの形成が必要不可欠になると考えています。各企業や組織が、これらのコミュニティから得られたノウハウを自分たちのセキュリティマネジメントサイクルにフィードバックし、さらに広げるといった、社会が「つながる」活動も、日立は積極的に推進しています。

2 新たなセキュリティ啓発活動　一人ひとりのセキュリティ意識こそが組織を守る砦（とりで）となる

昨今の新型コロナウイルス感染拡大により、私たちは新しい働き方を余儀なくされました。日立もテレワークの導入を一気に加速させ、在宅勤務を標準としたこれからの働き方を推進するための施策に取り組んでいます。

一方で、サイバー攻撃の脅威はますます高まっており、テレワークの推進には十分なセキュリティ対策が不可欠です。今まで攻撃者の主なターゲットは組織のITの脆弱性（ぜいじゃく）でしたが、テレワーク中心の働き方においては、「セキュリティ意識の脆弱性」が狙われることが想定されます。オフィス以外で仕事をすることにより、慣れない環境の中、つい気が緩んだり、近くに相談できる相手がいなかったりと、誰しもがリスクと隣り合わせになります。

そのために、これからは一人ひとりのセキュリティ意識の向上こそが最後の砦であると考え、私たちはITで守るセキュリティに加え、人で守るセキュリティ施策として、新たな視点で社員中心のセキュリティ啓発活動をスタートさせます。具体的には、従業員が自発的にセキュリティを学び、実践できる場を提供し、その教養を従業員同士が共有することで、さらに意識を高め合えるような活動を推進します。

3 協創によるこれからのセキュリティ

日立は、組織を守る大きな砦をつくるために、従業員一人ひとりがセキュリティを正しく理解し、あるべき姿に向かって働くことができる意識づくりをめざします。

また、社外への啓発活動などを通し、産・官・学が連携および協創した社会全体でのセキュリティエコシステムの構築を推進し、サイバーレジリエンス強化に取り組んでいきます。

新しい日常をより安全・安心で快適に過ごせるように、またそこに潜むリスクを回避できるように、日立はこれからも新しいセキュリティの取り組みを模索し、推進していきます。

日立グループにおけるCSIRT活動

日立インシデントレスポンスチーム（HIRT:Hitachi Incident Response Team）は、日立のサイバーセキュリティ対策活動を支援するCSIRT（Cyber Security Incident Readiness/Response Team）組織です。セキュリティインシデントの発生を予防し、万一発生した場合は迅速に対処することにより、お客さまや社会の安全・安心なネットワーク環境の実現に寄与します。

インシデントレスポンスチームとは

セキュリティインシデント（以下、インシデントと記す）とは、サイバーセキュリティに関係する人為的事象で、不正アクセス、サービス妨害行為、データの破壊などの行為（事象）を示します。

インシデントレスポンスチームは、組織間ならびに国際間の連携によって問題解決にあたるために、「技術的な視点で推し量り、伝達できること」「技術的な調整活動ができること」「技術面での対外的な協力ができること」という基本的な能力をもち、インシデントの予防（レディネス：事前対処）と解決（レスポンス：事後対処）を通じて、「インシデントオペレーション」を先導する組織です。

HIRTの活動モデル

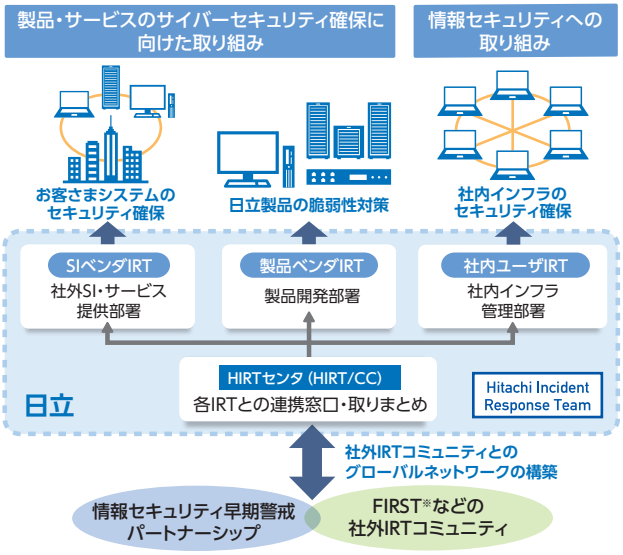
HIRTの役割は、「脆弱性対策：サイバーセキュリティに脅威となる脆弱性を除去するための活動」と「インシデント対応：発生しているサイバー攻撃を回避ならびに解決するための活動」を通じて、「組織単体活動：自身の企業情報システムを対象とする『情報セキュリティへの取り組み』」と「組織連携活動：お客さまの情報システムや制御システムを対象とする『製品・サービスのサイバーセキュリティ確保に向けた取り組み』」の視点から、日立のサイバーセキュリティ対策活動を支援していくことにあります。さらには、「次の脅威をキャッチアップする」過程の中で早期に対策の展開を図ることによって、安全・安心なインターネット社会の実現に寄与することにあります。

HIRTは、脆弱性対策とインシデント対応とを推進するために、下記のように、4つのIRT（Incident Response Team）という活動モデルを採用しています。4つのIRTとは、

(1) 情報システムや制御システム関連製品を開発する側面（製品ベンダIRT）
(2) その製品を用いてシステムの構築やサービスを提供する側面（SI [System Integration] ベンダIRT）
(3) インターネットユーザーとして自身の企業情報システムを運用管理する側面（社内ユーザIRT）

の3つとともに、

(4) これらのIRT間の調整業務を行うHIRT/CC（HIRTセンタ）を設け、各IRTの役割を明確にしつつ、IRT間の連携を図る効率的かつ効果的なセキュリティ対策活動を推進するモデルです。



分　類	役　割
HIRT/CC※	該当部署：HIRTセンタ FIRST、JPCERT/CC※、CERT/CC※などの社外IRT組織との連携、SIベンダ・製品ベンダ・社内ユーザIRT間の連携を通して脆弱性対策とインシデント対応活動を推進する。
SIベンダIRT	該当部署：SI・サービス提供部署 公開された脆弱性について、社内システムと同様にお客さまシステムのセキュリティを確保するなど、お客さまシステムを対象とする脆弱性対策とインシデント対応活動を支援する。
製品ベンダIRT	該当部署：製品開発部署 公開された脆弱性について影響の有無を迅速に調査し、該当する問題について、修正プログラムを提供するなど、日立製品の脆弱性対策を支援する。
社内ユーザIRT	該当部署：社内インフラ提供部署 日立サイトが侵害活動の基点とならないよう脆弱性対策とインシデント対応活動の推進を支援する。

※HIRT/CC：HIRT Coordination Center
FIRST：Forum of Incident Response and Security Teams
JPCERT/CC：Japan Computer Emergency Response Team/Coordination Center
CERT/CC：CERT Coordination Center
SI：System Integration

HIRTセンタが推進する活動

HIRTセンタの活動には、組織内IRT活動として、制度面を先導する情報セキュリティ統括部門と、品質保証部門との協力による制度・技術両面でのサイバーセキュリティ対策の推進、各事業部・グループ会社への脆弱性対策ならびにインシデント対応の支援があります。また、日立の対外的なIRT窓口として、組織間のIRT連携によるサイバーセキュリティ対策を推進しています。

●組織内IRT活動

組織内IRT活動では、セキュリティ情報の収集や分析を通じて得られたノウハウを注意喚起やアドバイザリとして発行するとともに、各種ガイドラインや支援ツールの形で製品・サービス開発プロセスにフィードバックします。

(1) セキュリティ情報の収集・調査分析・展開

情報セキュリティ早期警戒パートナーシップ※1の推進などを通じて、脆弱性対策ならびにインシデント対応に関する情報やノウハウを組織内に展開しています。

※1 ソフトウェア製品およびWebサイトに関する脆弱性関連情報の円滑な流通、および対策の普及を図るための、公的ルールに基づく官民連携体制

(2) 研究活動基盤の整備

「次の脅威のキャッチアップ」と早期に対策展開を図るための技術として「動的活動観測」に取り組んでいます。動的活動観測は、標的型攻撃などのサイバー攻撃を調査するために構築した組織内ネットワークの疑似環境下で、侵入後の攻撃者の行動を記録し分析する観測手法です。

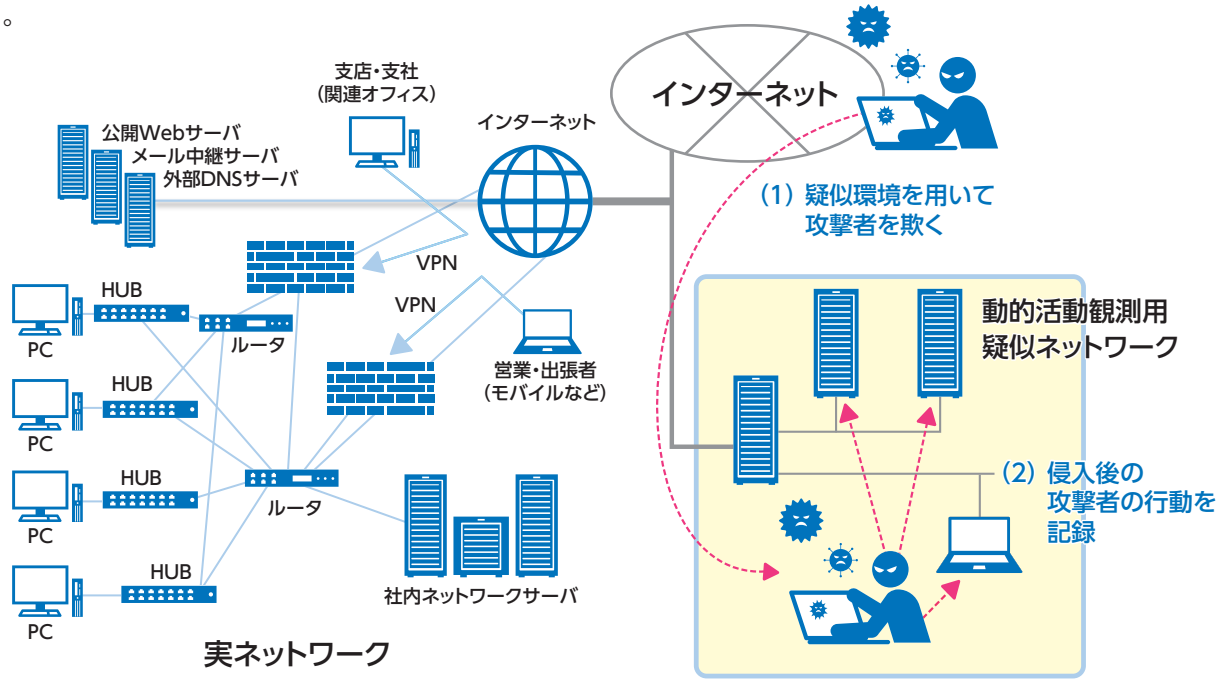
(3) 製品・サービスのセキュリティ技術の向上

組織的なIRT活動能力の向上にむけ、情報システムならびに制御システム関連製品に対するセキュリティ対策の具体化、エキスパート人財への技術継承を推進しています。また、実践的な社内セキュリティ啓発の一環として、標的型攻撃やランサムウェアなどのサイバー攻撃の疑似体験演習の開発にも取り組んでいます。

(4) 分野別IRT活動の実践

分野ごとの背景や動向を踏まえた対応を具体化していくため、分野に特化したIRT活動の検討と整備を進めています。金融分野における先行的な取り組みとして2012年10月に、HIRT-FIS※2を設置しました。

※2 HIRT-FIS:Financial Industry Information Systems



●組織間IRT活動

組織間IRT活動では、複数のIRTが協調して、新たな脅威に立ち向かうための組織間連携、互いのIRT活動の改善に寄与できる協力関係の構築を推進しています。

(1) IRT活動の国内連携の強化

日本シーサート協議会活動を活用して、情報収集において知り得た脆弱性やインシデント情報を他加盟組織のPoC (Point of Contact) に通知するなど、連携網の整備に努めています。また、JPCERTコーディネーションセンターと独立行政法人情報処理推進機構 (IPA) が共同運営するJVN※3を用いた情報利活用基盤の整備を支援しています。

※3 JVN:Japan Vulnerability Notes (脆弱性対策情報ポータルサイト)

(2) IRT活動の海外連携の強化

FIRST※4を通じた活動を活用した海外IRT組織ならびに海外製品ベンダIRTとの連携体制の整備、脅威情報構造化記述形式STIX※5、米国国土安全保障省のAIS※6などを用いた情報利活用基盤の整備を推進しています。

※4 FIRST:Forum of Incident Response and Security Teams
※5 STIX:Structured Threat Information Expression
※6 AIS:Automated Indicator Sharing

(3) 研究活動の整備

マルウェア対策研究人材育成ワークショップなど学術系研究活動への参画を通じて、人財育成の場の醸成、専門知識を備えた研究者や実務者の育成を推進しています。

■ Hitachi Incident Response Team

https://www.hitachi.co.jp/hirt/
https://www.hitachi.com/hirt/

サイバーセキュリティ対策

サイバー攻撃や各種セキュリティインシデントへ対応するために、日立では、社内で運営するセキュリティオペレーションセンター（SOC：Security Operation Center）を設置し、セキュリティ監視およびインシデント対応の強化、推進を図っています。

セキュリティ監視・インシデント対応強化

標的型攻撃の高度化、ファイルレスによる攻撃のステルス化、サプライチェーンのセキュリティリスクが懸念されるなど、近年、複雑化かつ巧妙化するサイバー攻撃により、企業や組織のセキュリティリスクが増大しています。このようなサイバー攻撃に対峙（たいじ）するためには、その脅威をいち早く発見し、被害拡大を防止することが重要です。

日立では、マルウェア感染や不正アクセスなどの脅威を早期に検知し、インシデント発生時の初動対応から対策までを迅速に実施し、サイバー攻撃に対する被害を最小限に抑えるための24時間365日体制のセキュリティオペレーションセンター（SOC）を2017年10月より設置し、セキュリティ監視・インシデント対応強化を図っています。

●セキュリティ監視

日立グループでは、対象とするシステムおよびネットワークの監視ポイントを定め、グローバルの各システムおよびネットワークデバイスのログの連携・監視を実施するログの統合監視・分析基盤の構築を行っています。また社内ネットワークでは監視ポイントを1つでも増やすことが早期検知につながるため、各部署管理の機器やシステムを棚卸しすることで、どこに何があるのか整理し、取得可能なログを確認し、検知に有用なものは新たに監視対象へと加えることで検知の早期化を実現しています。

監視の対象拠点として、2019年度は欧米、アジア、オセアニアなどにある日立グループにおける基幹拠点のログの統合監視・分析基盤の拡大を行いました。これにより、拠点ごとのログ監視がSOCに統合され、効果的かつ効率的にリスクの監視・早期検知を実現する環境を強化してきました。

さらに監視ポイントの強化も進めています。昨今のサイバー攻撃では、ファイルレスマルウェアやOS標準のツールが利用されるようになっており、シグネチャベースのアンチウイルスソフトで防ぎきることは不可能な状況です。侵入を防ぐだけでなく、侵入を前提とした対策が必要であることから、日立では、機器の動作の監視を行い、不審な挙動を検出し、調査・対処を実施するEDR（Endpoint Detection and Response）を導入し、エンドポイントの監視を強化しています。このほか、認証ログの監視や外部のセキュリティリスク評価サービスを用いた監視など、監視ポイントを広げています。

●インシデントレスポンス

インシデント発生に備えた対応手順、連絡体制を整備しており、インシデント発生時には、迅速にインシデントの原因究明や影響範囲の特定、事態の収束を行います。また、インシデントレスポンスから得られたノウハウを社内の各種セキュリティ施策にフィードバックし、インシデント再発防止を図る取り組みも実施しています。

2019年度は前述のグローバルにおけるログの統合監視・分析基盤の拡大を通して、現地サイバーセキュリティ担当者との関係を構築でき、インシデントの際のより迅速な対応を実現するスキームを確立しました。また、インシデントレスポンスで判明した攻撃者の攻撃行動や手口を積極的に他拠点の防御へ活かす活動を推進しています。

さらにEDRの導入により、侵害が確認された機器をネットワークから切り離して侵害拡大を防止する、不審な活動をしている機器を遠隔から調査する、といった対処を迅速に実施できるようになりました。従来グローバルなインシデントレスポンスでは時差により現地の担当者による即時の対処が難しい場合がありましたが、EDRの導入により24時間365日の初動対応を即座に実施することが可能になりました。

警戒情報の収集・分析・配信

日立製作所では、社内で利用している情報システムおよびお客さまへ提供する製品・サービスのセキュリティを確保するための活動として、警戒情報の収集・分析・配信を行っています。

この活動は、グループ会社とも連携して推進しています。

●脅威情報の収集・分析

脅威情報の収集では、以下に示すようなWeb上に公開されている脆弱性情報・脅威情報に加え、日立システムズ社をはじめとした各種CTIサービスを活用して、国内・海外含めたセキュリティ情報の収集を行っています。

- IPA、JPCERT/CC、USCERTなどの社外団体の発信サイト
- セキュリティ関連のニュースサイト
- 各種セキュリティベンダのブログサイト

収集した脆弱性情報・脅威情報については、情報元が公開している指標（深刻度、CVSS基本値など）から攻撃成功の可能性、社内システムでの利用状況などを考慮し、配信対象の選定・3段階の警戒レベルの判定を行っています。また、CTIサービスを利用して、脆弱性の悪用や脅威の深刻度、被害の発生状況などを見定め、分析に活用しています。

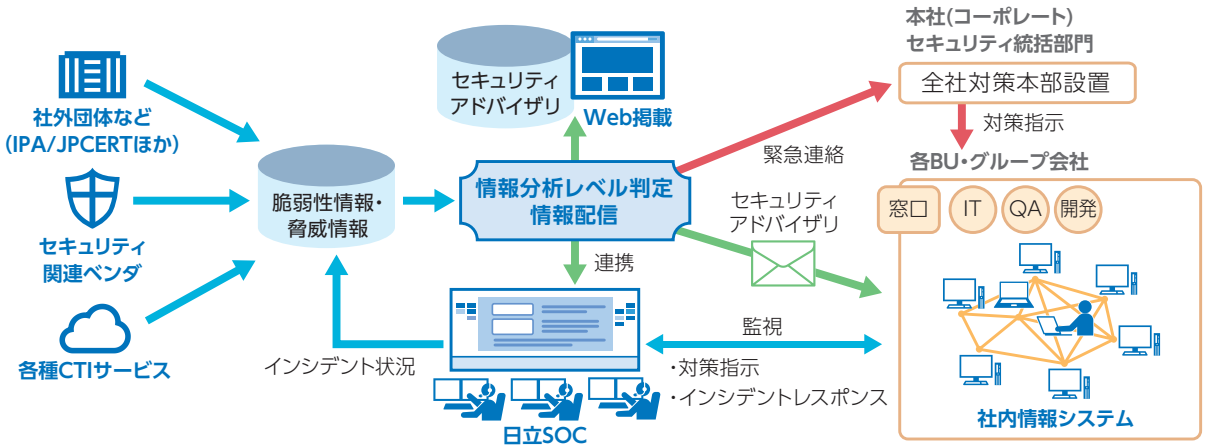
●セキュリティアドバイザリの配信

配信対象の情報は、警戒レベルに応じ、各BU・グループ会社から選出されたサイバーセキュリティ責任者に対して、即時～週次でのメール配信、社内Webへの掲載などのコミュニケーション手段を通じて周知を行っています。また、日立社内に関わる影響範囲の広い脅威に対しては、セキュリティアドバイザリで注意喚起を促すとともに、必要に応じてサイバー警報を発報し、日立グループ全社に対して対策強化を行っています。

2019年度からは、収集した情報を基に社内への影響が想定される脅威に対して、日立SOCや情報システム部門と連携し、セキュリティ機器での対策確認・監視強化を実施しています。また、発見した脅威に対して、社外に公開しているシステムの状況を調査し、影響のあるシステムについては該当部署へ個別に通知・対策を促す活動を行っています。

●緊急時の際の対応

社内の多数の拠点において重大な業務影響がある場合や、全社レベルで業務継続が不可能な場合には、全社対策本部を設置し、統括したセキュリティ対策指示を行います。



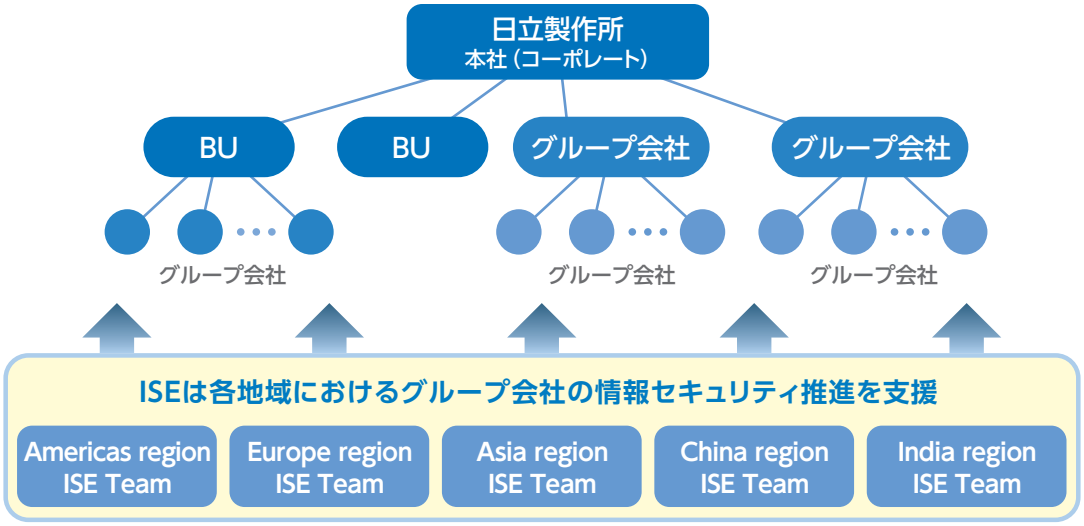
グローバル情報セキュリティの取り組み

グローバルビジネスの拡大に伴い全世界の日立グループにおいて、情報セキュリティの取り組みが重要となっています。日立では、セキュリティ施策の確実な遂行に向け、グローバルセキュリティにおけるガバナンス浸透を向上させるべく、各地域に情報セキュリティエキスパートを設置し、グローバルガバナンス強化に取り組んでいます。

グローバルセキュリティガバナンス

情報セキュリティのガバナンスラインは、日立グループのセキュリティ統括部門より方針・施策を各BU・グループ会社へ共有・指示を行い、各BU・グループ会社はそれぞれ区処する海外法人に対し、その実行を指示します。

グローバルで各社の情報セキュリティ推進を支援するため、2019年より各地域に情報セキュリティエキスパート（ISE:Information Security Expert）を設置し、ガバナンス浸透を向上させる活動を開始しました。2020年現在、米州、欧州、アジア、中国、インド地域に配置し、各地域の現地法人支援を行っています。



情報セキュリティエキスパートによるガバナンス強化活動

情報セキュリティエキスパート（ISE）は、セキュリティ統括組織と一体となり、各地域のガバナンス強化を図っています。

各地域でのコミュニティ確立、コミュニケーション活性化のためISEによるサイバーセキュリティワークショップやウェブセミナーを開催し、区処会社経由の本来のガバナンスルートを補完する機能として、現地法人へのガバナンス強化支援を行っています。

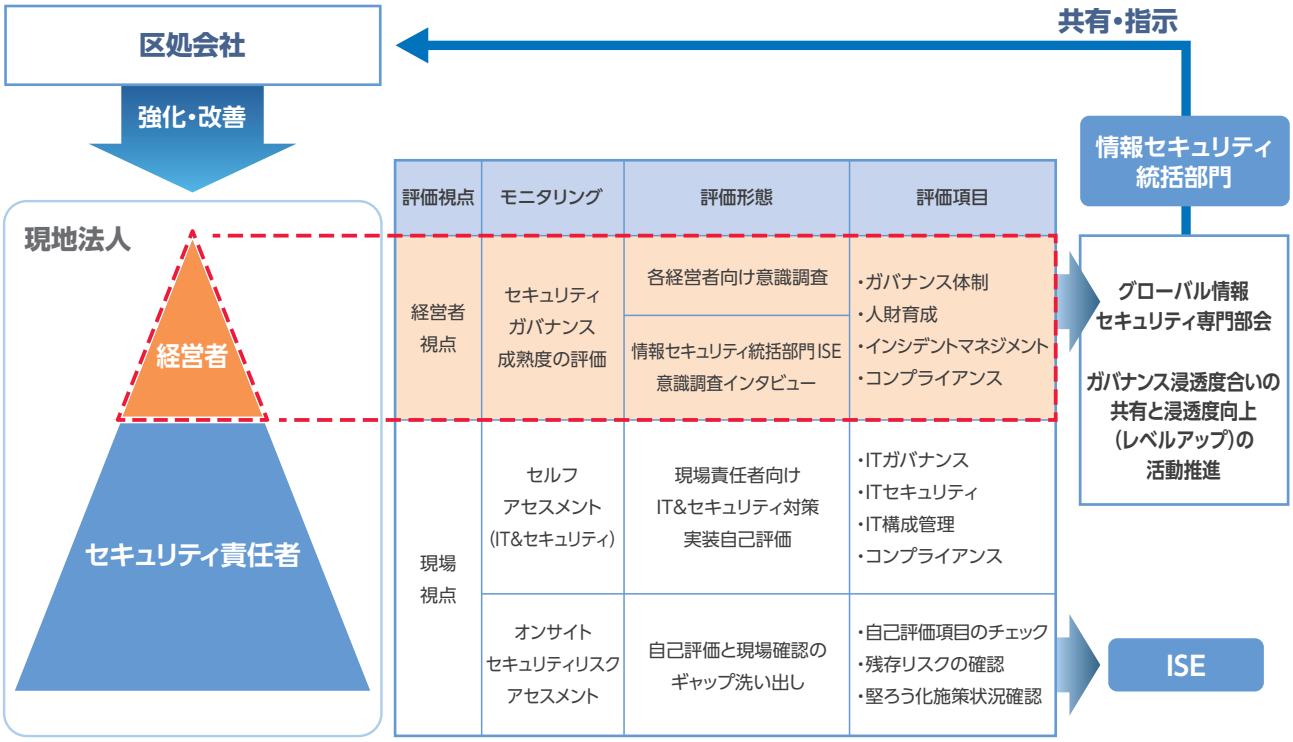
ISEの主な活動内容
1. セキュリティ統括組織と連携したセキュリティ施策計画策定・実行
2. セキュリティ成熟度・ガバナンス浸透度の把握と各社向上支援
3. 各地域におけるセキュリティコミュニティの確立
4. 海外現地法人のセキュリティ担当を対象としたワークショップの開催
5. 各地域における各種法律・規制への関係部署との連携対応
6. 最新動向把握のための社外カンファレンスなどへの参画

経営者意識調査の実施

日立グループでは、現場視点のIT&セキュリティ対策実施自己評価および第三者によるアセスメントを実施し、ITガバナンス向上を推進しています。

従来の現場視点に加え、経営者視点のセキュリティガバナンス成熟度を把握すべく、海外現地法人の経営者向けにセキュリティガバナンスの取り組み状況について意識サーベイを実施しています。

意識サーベイは、ガバナンス体制、人財育成、社内ITセキュリティ、生産・製造セキュリティ、製品セキュリティ、サードベンダ、コンプライアンスといった多方面をカバーする内容となってます。



サーベイ結果の可視化とPDCA活動

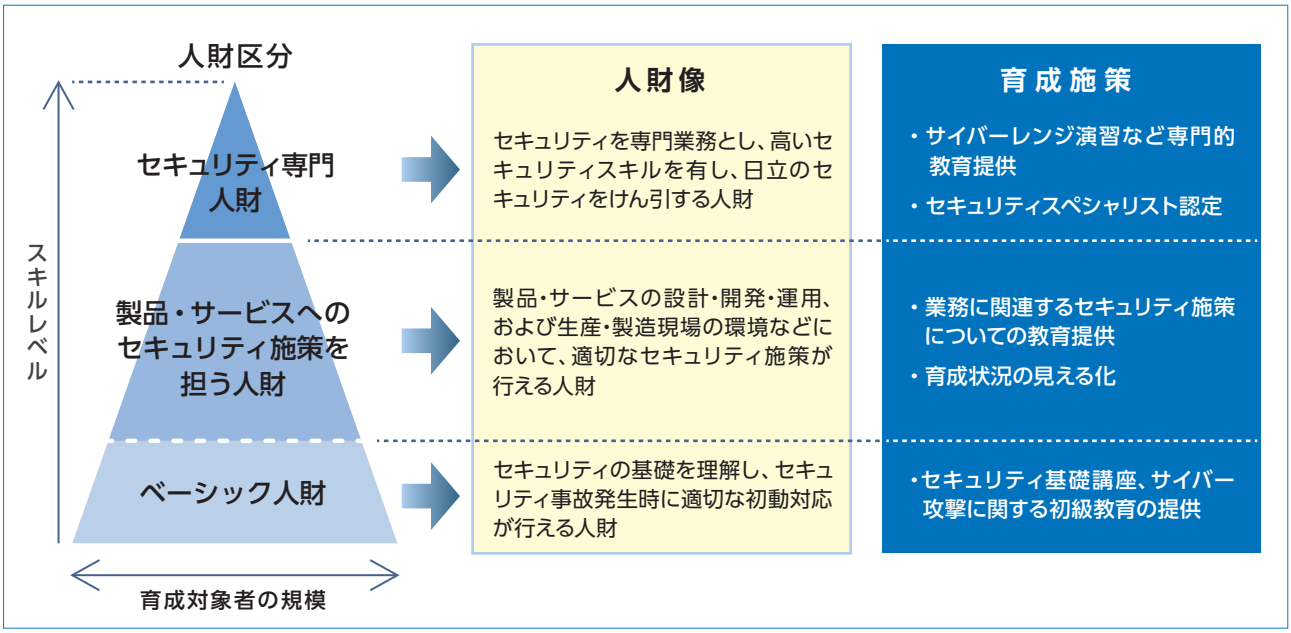
海外現地法人経営者向けのサーベイ結果については、データの可視化・分析を行い、ガバナンス浸透度を上げる具体的な活動立案につなげています。また、可視化されたデータについては、BU・グループ会社のセキュリティ管理・統制を行う責任者とも共有し、各社でのセキュリティ活動立案（Plan）、実施（Do）、確認（Check）、評価・改善（Action）の指標としても有効利用を図っています。

セキュリティ人財育成の取り組み

日立グループでは、お客さまに提供する製品・サービスにおけるセキュリティ対応を適切に行うために、人財に対するセキュリティの観点での育成を全社において推進しています。

近年のサイバー攻撃の激化に伴い、日立グループでは、お客さまに提供する製品・サービスのセキュリティ確保を目的に、それらを提供する人財へのセキュリティ観点での育成を推進しています。育成する人財は、右の3つに分類されます。高度なセキュリティ専門家だけでなく、製品・サービスの開発・運用に携わる技術者や社内ITの利用者も対象として人財育成を進めています。

- 高いセキュリティスキルを持ち、日立グループのセキュリティをけん引するセキュリティ専門人財
- お客さまへ提供する製品・サービスの設計・開発・運用、および生産・製造現場のセキュリティ施策を担う人財
- セキュリティの基礎を理解し、セキュリティ事故発生時に適切に対応できるベーシック人財



セキュリティ専門人財向けには、サイバーレンジ演習などのハイレベルの教育提供、セキュリティ専門人財間の情報共有・連携を支援するコミュニティサイトの運営などを行っています。また、セキュリティ専門人財を認定する仕組みとして、2014年8月より、一般社団法人情報処理学会「認定情報技術制度」の企業認定に準拠した日立ITプロフェッショナル認定制度（Hitachi Certified IT Professional）を創設し、運営しています。この制度の下、情報セキュリティスペシャリスト（HISSP:Hitachi Certified Information Security Specialist）として、必要なセキュリティスキルとキャリア（業務実績など）を備えたセキュリティ専門人財を発掘・育成・評価し、これまでに1,000名を超える人財を認定しています。

製品・サービスへのセキュリティ施策を担う人財とは、製品・サービスの提供という業務を推進する中で、必要なセキュリティ施策を推進する人財です。まず、製品・サービスの設計・開発・運用保守、それら業務の環境整備などにおいて、セキュリティ施策を適切に行う人財の育成です。また、生産・製造の現場にフォーカスしたセキュリティ人財の育成も重要です。これら人財に対しては、社内規定などで示されたセキュリティ施策の理解を促進するための教育を提供しています。製品・サービスの設計・開発と生産・製造現場はそれぞれ安全を確保しつつお互いに悪い影響を及ぼさぬよう環境を構築・運用しなければならないため、IT/OTに関わるセキュリティ対策を実施するためのさまざまなスキルアップに取り組んでいます。

ベーシック人財の育成は、全社におけるセキュリティ意識を底上げし、セキュリティ対応を強化することを目的に、職場の担当者など多くの人財を対象とするものです。セキュリティの基礎知識に加え、サイバー攻撃といったセキュリティ事故発生時の適切な初動対応について修得することを目的に育成を行います。ベーシック人財向けの教育としては、2016年度より提供を開始した「サイバー攻撃対応基礎知識修得eラーニング」教育と「サイバー攻撃対応コミュニケーション訓練」教育があり、これまでに4,500名を超える人財が受講をしています。また、さらなる導入教育が必要な人財向けに、セキュリティ基礎知識に関するeラーニング教育なども提供しています。

なお、2020年度は、新型コロナウイルスによる環境の変化に対応し、集合教育として提供していた教育のオンライン化を推進しています。ベーシック人財向けにワークショップ形式で提供していた「サイバー攻撃対応コミュニケーション訓練」についてもオンライン教育へ移行しています。

サイバー攻撃対応基礎知識修得eラーニング

✓サイバー攻撃を受けた際の動きや影響を修得する研修

【基礎知識】
①日常業務での注意点、②サイバー攻撃への対処、③開発時の注意点、
④脆弱性情報の収集と対策検討、⑤インシデント発生時の備え

【体験学習】
①標的型攻撃による情報流出、②ランサムウェア感染による業務妨害、
③Webアプリケーションの脆弱性による被害、④マルウェア被害

サイバー攻撃対応コミュニケーション訓練（ワークショップ）

✓インシデント発生時の状況把握、対応内容決定の訓練

【対応プロセス】
①Observe（観察）、②Orient（方向付け）、③Decide（意思決定）、
④Act（対応・対策）に要求される迅速性、正確性の体験

【コミュニケーションスキル】
①報告、②連絡、③相談において、役割分担の重要性や出来事を5W1Hで正確に伝えることの重要性の理解

サイバーセキュリティマネジメントの取り組み

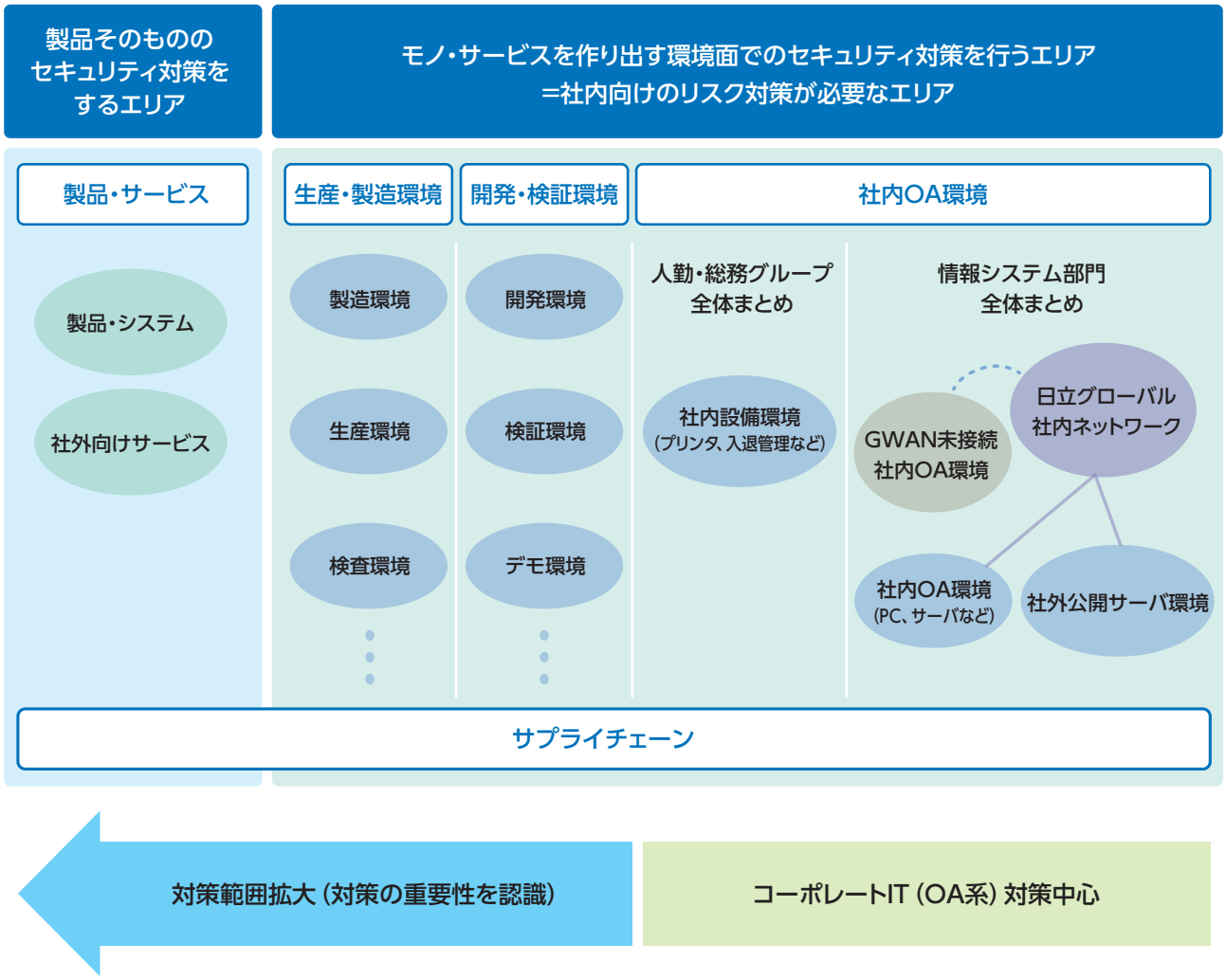
サイバー攻撃手法の多様化に伴い、インシデントの発生源や影響が拡大する中、こうしたリスクに対応するため、今までのOAで利用する社内IT環境の対策が中心であったセキュリティリスクのマネジメント範囲を拡大し、製品・サービスを作り出すための開発・生産・製造環境、サプライチェーンや製品・サービスの開発プロセスに対しても対象を広げ、事業のリスク低減に取り組んでいます。

背景と目的

2017年5月、製造現場の検査機器がランサムウェア(Wanna Cry)に感染し、日立グループ全体に被害が拡大しました。

この教訓から、ITが、生産・製造、開発試験などの事業の現場に浸透していく中、従来のOA環境以外の攻撃への対応、また、製品・サービスや調達に対するサイバーセキュリティ対策が求められるようになってきました。

このため、2018年から、社内OA、開発・検証、生産・製造の環境系のサイバーセキュリティ対策と、製品・サービスやサプライチェーンにおけるプロセス系のサイバーセキュリティ対策強化に取り組んでいます。

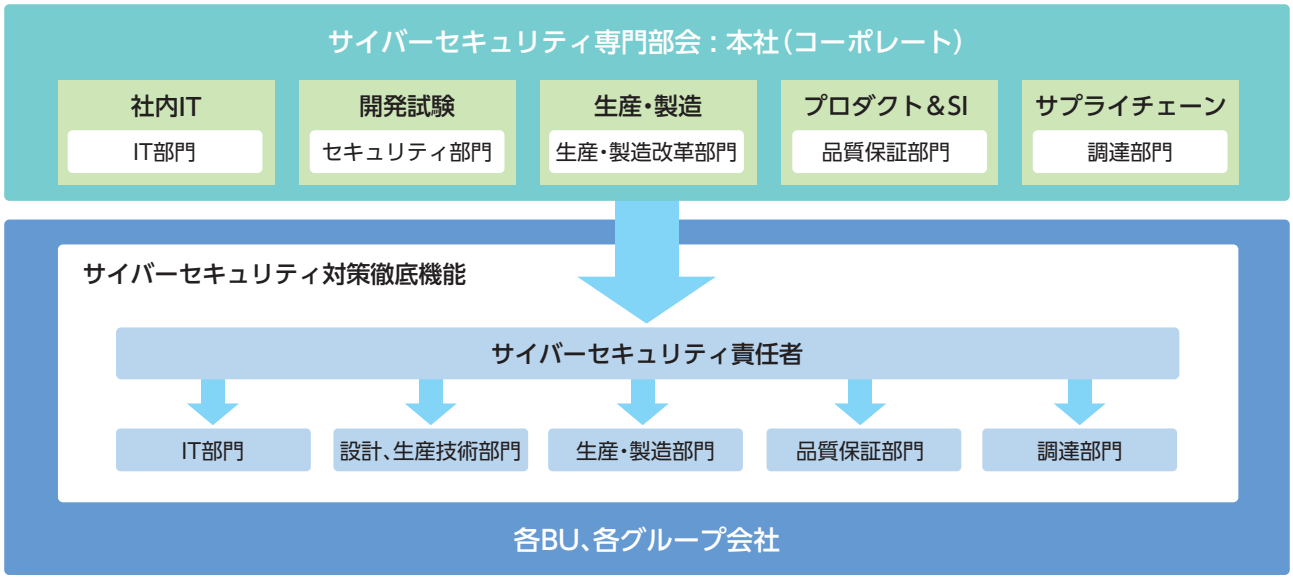


推進体制

本社（コーポレート）では、サイバーセキュリティ専門部会内に各領域別に分科会を設置し、サイバーセキュリティの強化施策を立案します。

各分科会での施策は、サイバーセキュリティ専門部会から、グループ内の各BU・グループ会社のサイバーセキュリティ対策徹底機能の取りまとめであるサイバーセキュリティ責任者を通じて、各部門へ展開されます。

各部門は、サイバーセキュリティ責任者の指示に基づいてサイバーセキュリティ対策に対する施策の周知徹底を図ります。



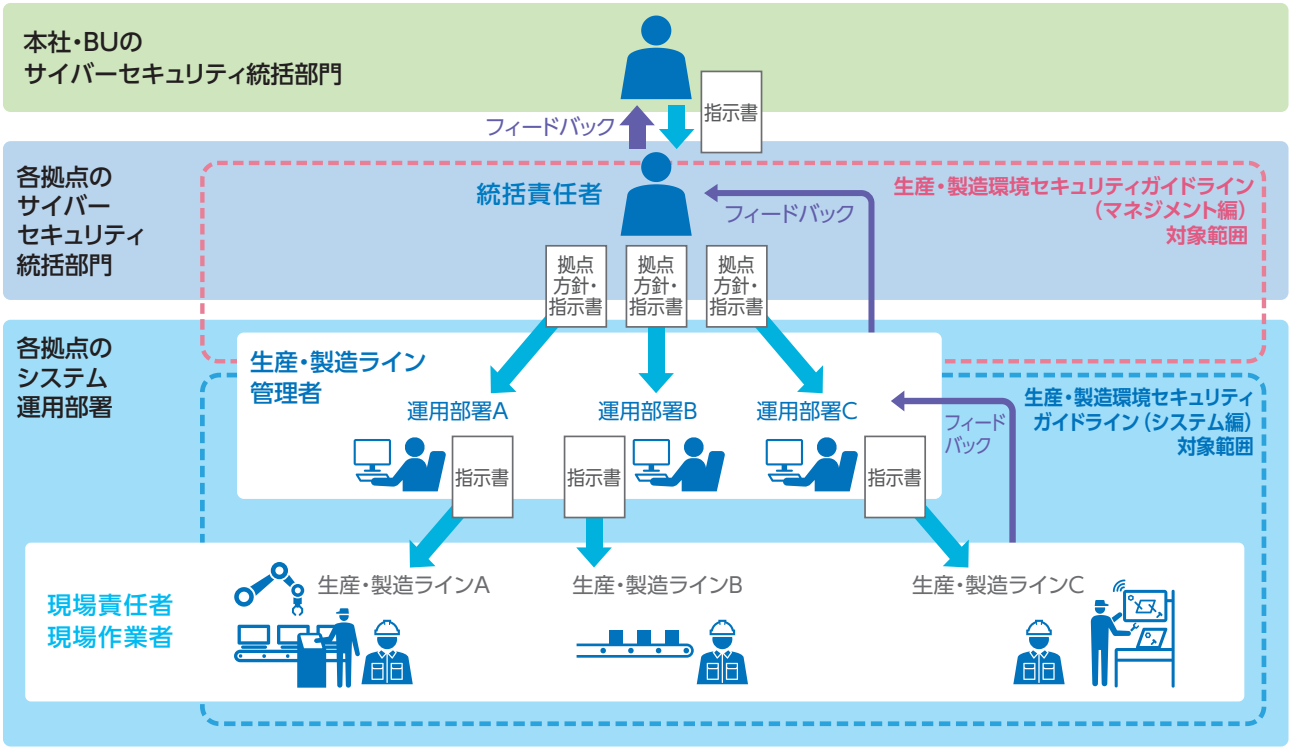
サイバーセキュリティ対策の強化施策

各領域のサイバーセキュリティ対策の強化について、下表の取り組みを進めています。

領域		対象部門	取り組み概要
社内OA	環境面	IT	・社内OA環境の接続・分離要求事項の策定と展開
開発・試験		設計・開発	・社内OA環境と安全な接続環境の構築ガイドラインの策定と展開
生産・製造		生産・製造	・制御システムをサイバー攻撃から守るための汎用的な標準規格であるIEC62443をベースとした生産・製造環境の構築ガイドラインの策定と展開
製品・サービス	プロセス面	設計・開発 品質保証	・製品・サービスのセキュリティ品質マネジメント指針の策定 ・製品の設計、開発・保守の各プロセスの要求事項策定と展開
サプライチェーン		調達	・取引先パートナーへのサイバーセキュリティ対策の要求事項の策定と評価プロセスに基づいた評価

●生産・製造現場におけるセキュリティ強化の取り組み

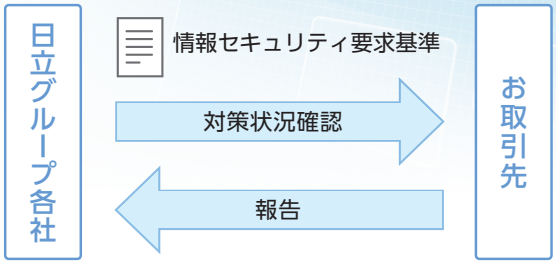
生産・製造環境は、他環境（社内OA、開発など）と相互に影響を与えない、受けないようにするため、相互の安全な接続環境の構築および運用管理についてガイドラインを整備し、日立グループ内でガイドラインに基づいた対応を進めています。また、実際の生産・製造現場においては、現場作業員の日々の作業において、順守すべき項目をポスターやルール集などの啓発コンテンツの展開を行い、現場のセキュリティ意識を高めています。



ガイドライン構成	内　容	対象者
マネジメント編	マネジメント面（組織・人的管理面としての取り組み）として、組織体制の整備および、拠点全体・部署個別のセキュリティ運用・管理上ルールの策定と見直しについて記載。	サイバーセキュリティ統括責任者
システム編	「IEC62443-3-3」に基づき、現状把握と対策検討としてシステム構成およびその対策方法は、日立グループの代表的なモデルを用いて記載し、各部門・各部署でカスタマイズして利用する。	生産・製造ライン管理者 現場責任者 現場作業者

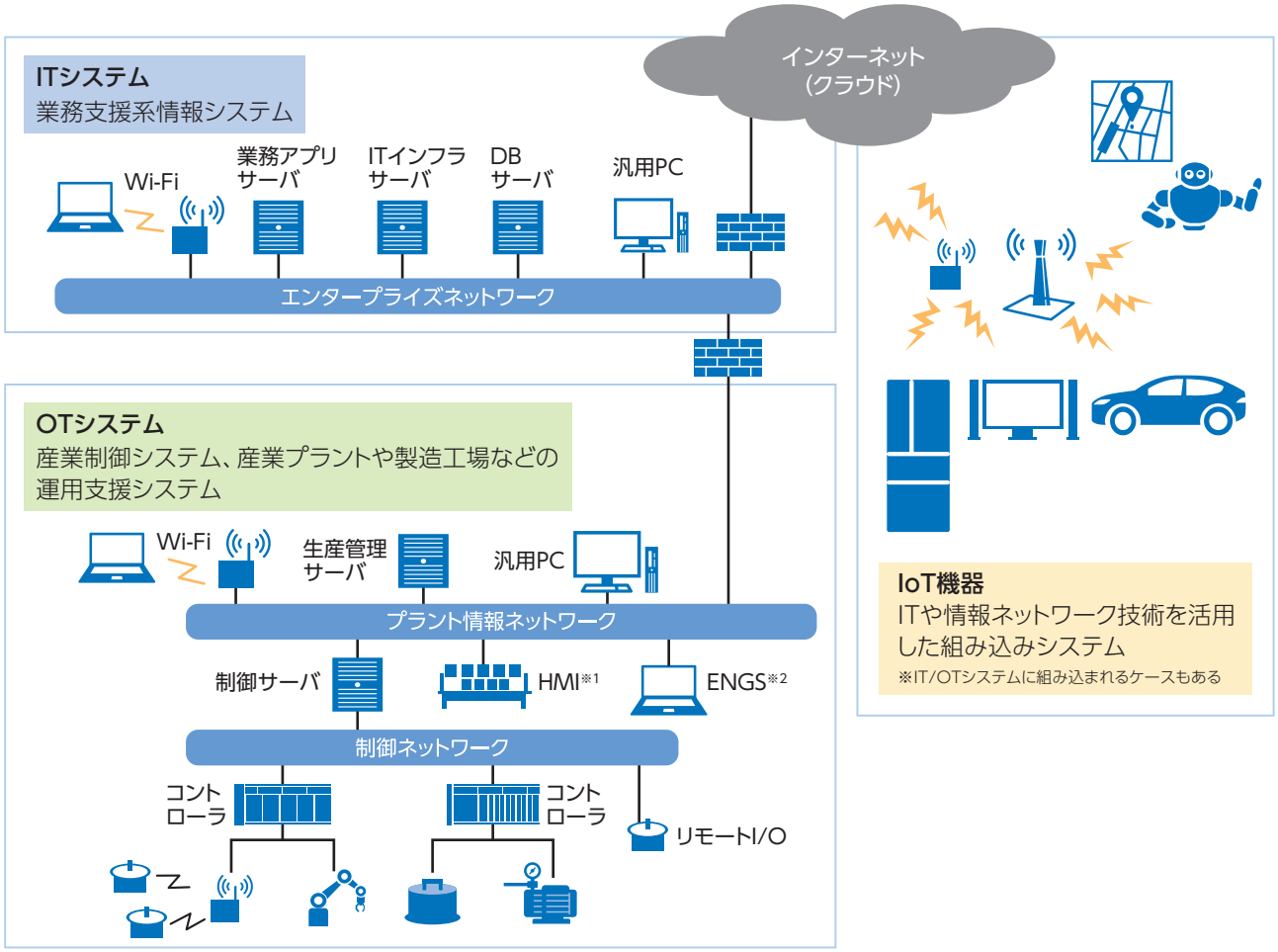
●サプライチェーンにおけるセキュリティ強化の取り組み

業務を委託する際には、あらかじめ日立が定めた情報セキュリティ要求基準に基づき、お取引先の情報セキュリティに関する対策状況を確認、審査しています。この情報セキュリティ要求基準には、昨今のサプライチェーンに対するサイバー攻撃に対するセキュリティ対策の項目を付加した「情報セキュリティガイドライン」を追加し、日立の情報セキュリティに関する要求を具体的に示し、お取引先へ確認頂いています。



製品・サービスに関するセキュリティの取り組み

デジタルソリューション事業の推進において、デジタル化やネットワーク化といった技術の高度化やシステムのオープン化によって新たな顧客価値を提供する一方で、サイバーセキュリティリスクとその対応の重要性も増しています。日立グループが提供するITシステム・OTシステム・IoT機器といった幅広い分野の製品・サービスでは、サイバー攻撃からお客さまの資産や社会インフラを守るための取り組みを継続的に進めています。



※1 Human Machine Interface　※2 Engineering Station

●製品・サービスに関するセキュリティマネジメント指針

日立グループの多種・多様な製品・サービスに対して、セキュリティマネジメントに関する考え方の統一を図るために、「製品・サービスに関するセキュリティマネジメント指針」と関連文書を品質保証規程として作成しています。

各部門は、セキュリティマネジメントに関する部門規則類に指針の内容を反映することにより、製品・サービスの開発・製造・保守・運用などのライフサイクルに渡るセキュアプロセスの実装を推進しています。

規定等の文書	概　要
製品・サービスに関するセキュリティマネジメント指針	日立グループ内における製品およびサービス（以下、製品と記す）のセキュリティマネジメントに関する考え方の統一を図ることを目的とした指針。
製品の開発・保守の各プロセスへの要求事項	製品の開発・保守プロセスへの要求事項。製品の特性に応じて要求事項を具体的なタスクに展開し、必要に応じてチェックリスト等を整備する。
製品セキュリティ点検チェックリスト	自部門の製品開発・保守プロセスが指針および要求事項に準拠しているかを確認するための点検チェックリスト。

●ガイド類の展開とサポート活動

各部門がセキュリティマネジメントに関する部門規則類を整備する際の参考資料として、「セキュアプロセス実装ガイド」をはじめとする各種ガイド類を展開しています。これらにおいて、設計・製造、運用・保守、セキュリティインシデントの各プロセスでの実装手順等について、セキュリティ対策が先行している部門の取り組みを実践事例として、日立グループ全体でノウハウの蓄積と共有を図っています。

これらのガイド類をイントラネットで共有するとともに、各部門でのセキュア開発プロセスの構築をサポートする活動を行っています。

1.設計・製造プロセス	2.運用・保守プロセス	3.セキュリティインシデント対応プロセス
1-1. リスク分析・要件定義/基本設計	2-1. 変更管理	3-1. 社内で検知した場合
1-2. 構成管理	2-2. 脆弱性情報の収集	3-2. 社外で検知した場合
1-3. 設計/製造	2-3. 予防保守	3-3. 定期訓練
1-4. 調達（OSS含む）	2-4. 定期脆弱性点検	
1-5. テスト/評価	2-5. 脆弱性および対策情報の顧客への告知	
1-6. 検査		

●製品・サービスのセキュリティ確保に関する先行的な取り組み

日立製作所では、お客さまへ提供する情報系製品・サービスのセキュリティを確保するため、セキュリティ対応施策の検討・策定体制を有し、セキュリティマネジメントプロセスに沿ってそれらを運用、改善する活動を推進しています。その長い歴史の中で、先行的に実施している取り組みについて、以下に記します。

(1) セキュリティ対応施策の策定・運用

セキュリティ対応施策の策定・運用を推進しています。例えば、インターネットへの接続は一般に高いリスクを伴うことから、インターネット接続に対する認可制度を設けており、承認を得なければインターネットへの接続や公開などが行えない仕組みをとっています。本活動には、関連するグループ会社も参画しており、連携して策定された施策は、関連する事業部門に展開され、各事業部門において運用されます。

(2) セキュリティマネジメントプロセスに沿った製品・サービスの開発・運用

製品・サービスの開発・運用の各フェーズに、セキュリティマネジメントプロセスを定義し、それを規則化することで組織におけるセキュリティ対策の確実な実施につなげています。リスクの大小を定義するセキュリティランクの概念を採用し、ランク付けの指標を定義し、セキュリティランク別に開発・運用時のセキュリティ確保に必要なセキュリティマネジメントプロセスを示しています。セキュリティランクの採用は、リスクの高さを認識し適切な対応をとることを促すだけでなく、リスクとコストのバランスの考慮にもつながります。またそのプロセスは、日立において標準化されている情報システム開発プロセスとも連携した内容となっています。規則化されたセキュリティマネジメントプロセスの内容は、定期にまたは必要に応じて随時に改訂されます。これは、発生したインシデント、顕在化したリスク、運用した結果などからのフィードバックに基づき実施され、マネジメントプロセスがより適切なものになるよう継続的な改善を行うことを目的としています。

(3) 脆弱性点検の実施

脆弱性攻撃による被害の抑止を目的に定期的脆弱性診断を実施しています。点検のタイミングは、新規開発時、環境変更時および定期実施としています。点検方法は、チェックリストを用いた定性的なものと、脆弱性点検ツールを用いたものがあり、これらを単独または併用することで、システム特性や運用状況に沿った適切な点検が行えるようにしています。

(4) 脆弱性関連情報のハンドリングとインシデント対応体制の整備

脆弱性を悪用したセキュリティインシデントの発生可能性の低減を目的に、情報系製品・サービス提供部門における脆弱性関連情報のハンドリグプロセスをガイドにまとめ、これに基づき活動を推進しています。また、大規模なインシデント発生時の対応体制および対応マニュアルを整備、訓練を実施することで迅速かつ的確な対応ができるよう備えています。

個人情報保護に対する取り組み

デジタルテクノロジーの進展に伴いデータの利活用が急速に進む中、個人情報保護への関心も高まっています。EUをはじめ130以上の国と地域が個人情報に関する権利保護を目的とした法律を制定しています。
そのような環境の中、安全・安心な社会インフラシステムを提供する日立は、お客さまからお預かりした個人情報や、事業運営に関わる個人情報を確実に管理するため、個人情報保護の取り組みを重視してます。「安心・信頼を提供する」、「個人の権利を大切にする」という個人情報保護に関するビジョンを定め、グローバル社会の一員として個人情報保護に取り組んでいます。

個人情報保護ガバナンスのビジョン

VISION

グローバル社会の一員として個人情報保護に取り組む

1 安心・信頼を提供する

- 法令などに適合した個人情報保護・機密情報管理プログラム（プロセス規定）の順守により、事業に取り組み、安心・信頼を提供してまいります。

2 個人の権利を大切にする

- グローバル全体の動向である個人の権利尊重に対して、日立として誠実に向き合います。
- 「個人情報保護」は基本的人権の尊重であり、日立での経営の重要イシューとして取り扱います。

日立の個人情報保護のビジョンとして、1 安心・信頼を提供する、2 個人の権利を大切にすることを掲げ、個人情報保護を経営の重要イシューとして位置づけ、着実に推進しています。

個人情報保護方針

日立製作所は個人情報保護方針を制定し、ホームページに掲載するなど広くステークホルダーに公表しています。
(http://www.hitachi.co.jp/utility/privacy/index.html)

●個人情報保護に関する当社の考え方

日立製作所（以下、当社と記す）は、トータルソリューションを提供できるグローバルサプライヤーとして、当社の技術情報や、お客さまからお預かりする情報をはじめさまざまな情報を取り扱っております。このことから、当社ではこれら情報価値を尊重するために、情報管理体制の確立とその徹底に努めて参りました。

●個人情報保護方針

(1) 個人情報管理規則の策定および個人情報保護マネジメントシステムの継続的改善

当社は、役員および従業員に個人情報保護の重要性を認識させ、個人情報を適切に利用し、保護するための個人情報管理規則を策定し、個人情報保護マネジメントシステムを着実に実施します。更に、維持し、継続的に改善します。

(2) 個人情報の収集・利用・提供および目的外利用の禁止

当社は、事業活動において、個人情報をお預かりしていることを考慮し、それぞれの業務実態に応じた個人情報保護のための管理体制を確立すると共に、個人情報の収集、利用、提供において所定の規則に従い適切に取扱います。また、目的外利用は行わない、およびそのための措置を講じます。

(3) 安全対策の実施並びに是正

当社は、個人情報の正確性および安全性を確保するため、情報セキュリティに関する諸規則に則り、個人情報へのアクセス管理、個人情報の持ち出し手段の制限、外部からの不正アクセスの防止等の対策を実施し、個人情報の漏洩、滅失またはき損の防止に努めます。また、安全対策上の問題が確認された場合など、その原因を特定し、是正措置を講じます。

(4) 法令・規範の遵守

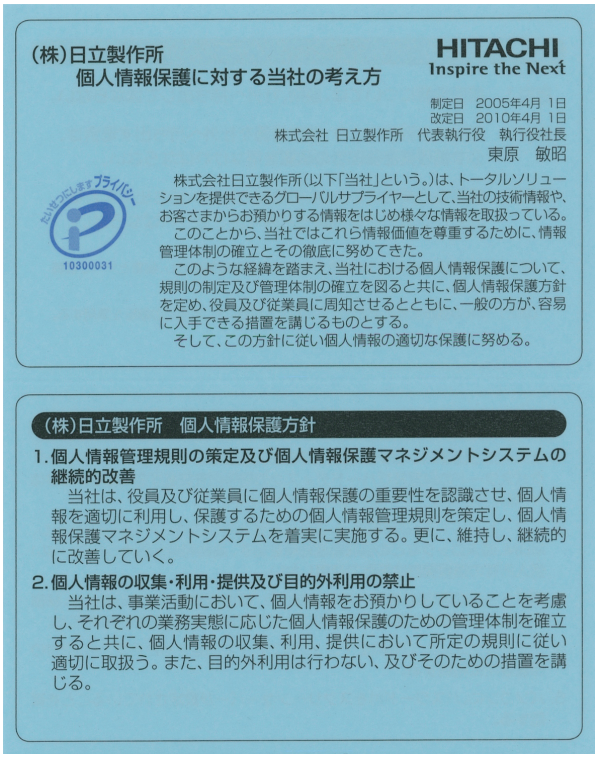
当社は、個人情報の取扱いに関する法令、国が定める指針その他の規範を遵守します。また、当社の個人情報管理規則を、これらの法令および指針その他の規範に適合させます。

(5) 個人情報に関する本人の権利尊重

当社は、個人情報に関して本人から情報の開示、訂正もしくは削除、または利用もしくは提供の拒否を求められたとき、および苦情、相談の申し出を受けたときは、個人情報に関する本人の権利を尊重し、誠意をもって対応します。

個人情報保護カード

日立製作所では、個人情報保護方針および情報セキュリティの基本事項を従業員に周知するために、個人情報保護カードを作成し、従業員一人ひとりに配布しています。



(株)日立製作所
個人情報保護に対する当社の考え方

HITACHI
Inspire the Next

制定日　2005年4月 1日
改定日　2010年4月 1日
株式会社 日立製作所　代表執行役　執行役社長
東原　敏昭

株式会社日立製作所(以下「当社」という。)は、トータルソリューションを提供できるグローバルサプライヤーとして、当社の技術情報や、お客さまからお預かりする情報をはじめ様々な情報を取扱っている。
このことから、当社ではこれら情報価値を尊重するために、情報管理体制の確立とその徹底に努めてきた。
このような経緯を踏まえ、当社における個人情報保護について、規則の制定及び管理体制の確立を図ると共に、個人情報保護方針を定め、役員及び従業員に周知させるとともに、一般の方が、容易に入手できる措置を講じるものとする。
そして、この方針に従い個人情報の適切な保護に努める。

10300031

(株)日立製作所　個人情報保護方針

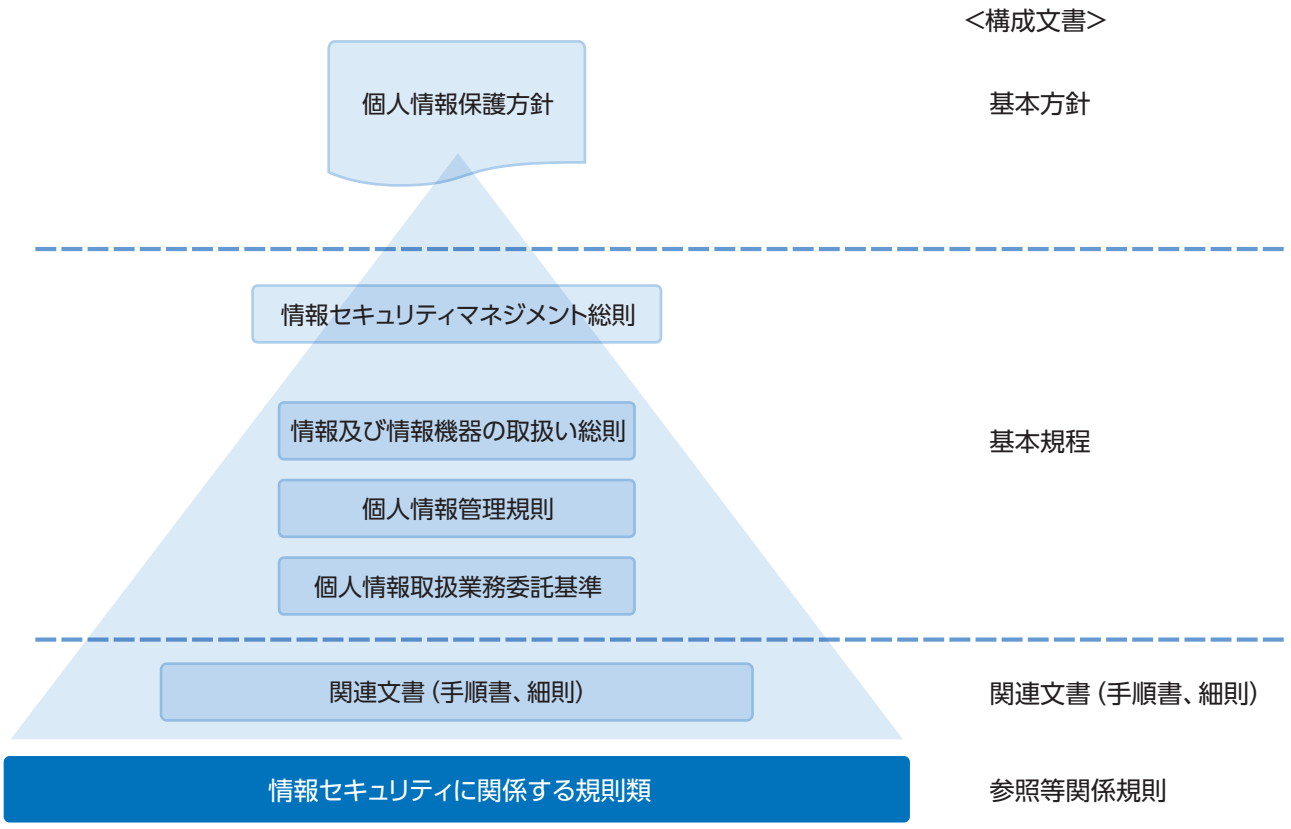
1. 個人情報管理規則の策定及び個人情報保護マネジメントシステムの継続的改善
当社は、役員及び従業員に個人情報保護の重要性を認識させ、個人情報を適切に利用し、保護するための個人情報管理規則を策定し、個人情報保護マネジメントシステムを着実に実施する。更に、維持し、継続的に改善していく。
2. 個人情報の収集・利用・提供及び目的外利用の禁止
当社は、事業活動において、個人情報をお預かりしていることを考慮し、それぞれの業務実態に応じた個人情報保護のための管理体制を確立すると共に、個人情報の収集、利用、提供において所定の規則に従い適切に取扱う。また、目的外利用は行わない、及びそのための措置を講じる。

個人情報保護体制

個人情報保護に関するビジョンを実現するため情報セキュリティに関する全社体制を構築しています。
詳細は「情報セキュリティ推進体制」をご参照ください。

個人情報規則体系

お預かりした個人情報は、個人情報保護規則する規則群に従って、適切に管理いたします。



個人情報保護マネジメントシステム

日立の個人情報保護マネジメントシステムはJIS Q 15001に準拠して定められています。個人情報保護に関する方針は個人情報保護方針として定めています。

個人情報保護のマネジメントの規則は、43条で規定される情報セキュリティマネジメント総則で定めています。

個人情報の取り扱いに関しては、63条で規定される個人情報保護規則および12条で規定される個人情報取扱業務委託基準、および関連文書に規定されています。

個人情報保護マネジメントサイクル

日立の個人情報保護マネジメントは、定期的にPDCA (Plan-Do-Check-Action) サイクルで実施するフレームワークで、計画を確実に実施し継続して改善していく仕組みを構築しています。

Planでは、個人情報保護方針、個人情報保護施策の策定、個人情報保護教育計画、個人情報保護監査計画を立案し、代表者である社長が承認します。

Doでは、個人情報保護施策の社内への展開と運用を行います。

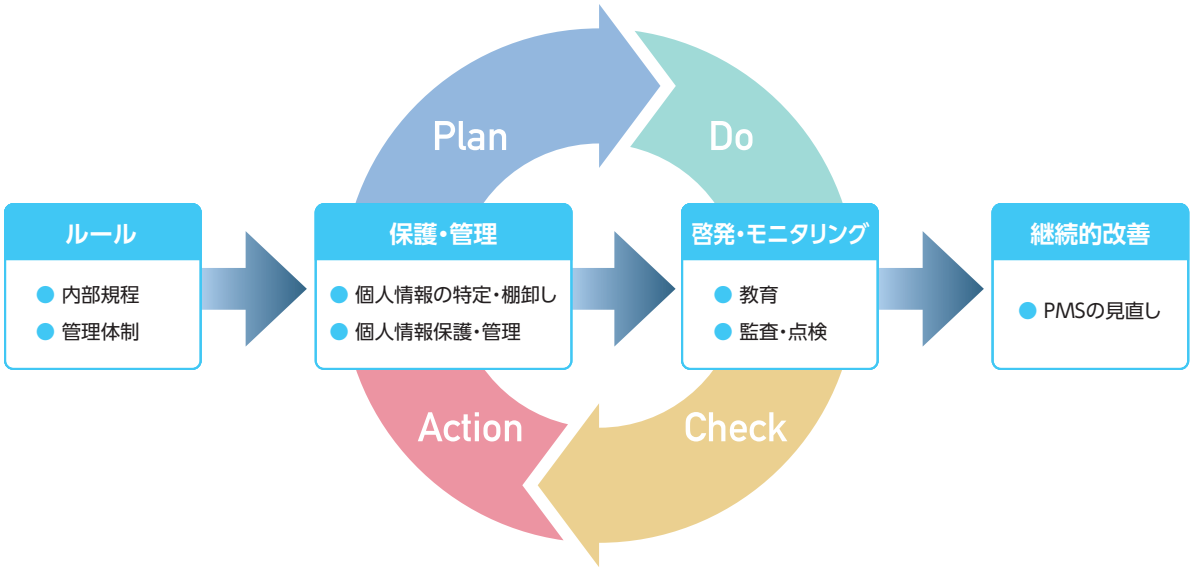
個人情報保護教育を実施し、個人情報保護施策や管理方法の周知徹底を図ります。(「個人情報の管理と適切な取り扱い」を参照)

また、個人情報保護に関する推進会議を開催し、各所への情報提供と施策の実施状況をフィードバックします。

Checkでは、全部署に対し、セルフチェックによる定期的な運用の確認、監査計画にのっとり他部署の状況を確認する監査を実施します。全社監査計画書、報告書は、監査責任者が策定し社長が承認します。指摘事項がある場合は、是正が完了するまで確認します。(「個人情報保護に関する監査」を参照)

Actionでは、個人情報の取り扱いに関する法令などの改正状況、社会情勢の変化、社内外から寄せられた意見、事業領域の変化といった経営環境の変化、社内運用状況の結果などに基づいてマネジメントシステムの見直しを行っています。

- 日立個人情報保護マネジメントシステム (PMS) の着実な実行
- PDCAを回し、定期的見直し、継続的改善を実行



個人情報保護のフレームワーク

日立では、個人情報の適正な取り扱いの確保について組織として取り組むために、トップマネジメントが個人情報保護方針を策定、この基本方針に従った個人情報管理規則やガイドラインなどの社内規定を策定しています。また、社内規程が法令、プライバシーマーク準拠規程であるJIS Q 15001に適合しているかを確認、評価する仕組みを整備しています。このような規程の整備とともに、実際に個人情報を取り扱うにあたり、4つの側面（組織的、人的、物理的、技術的）から具体的な安全管理措置を講じています。

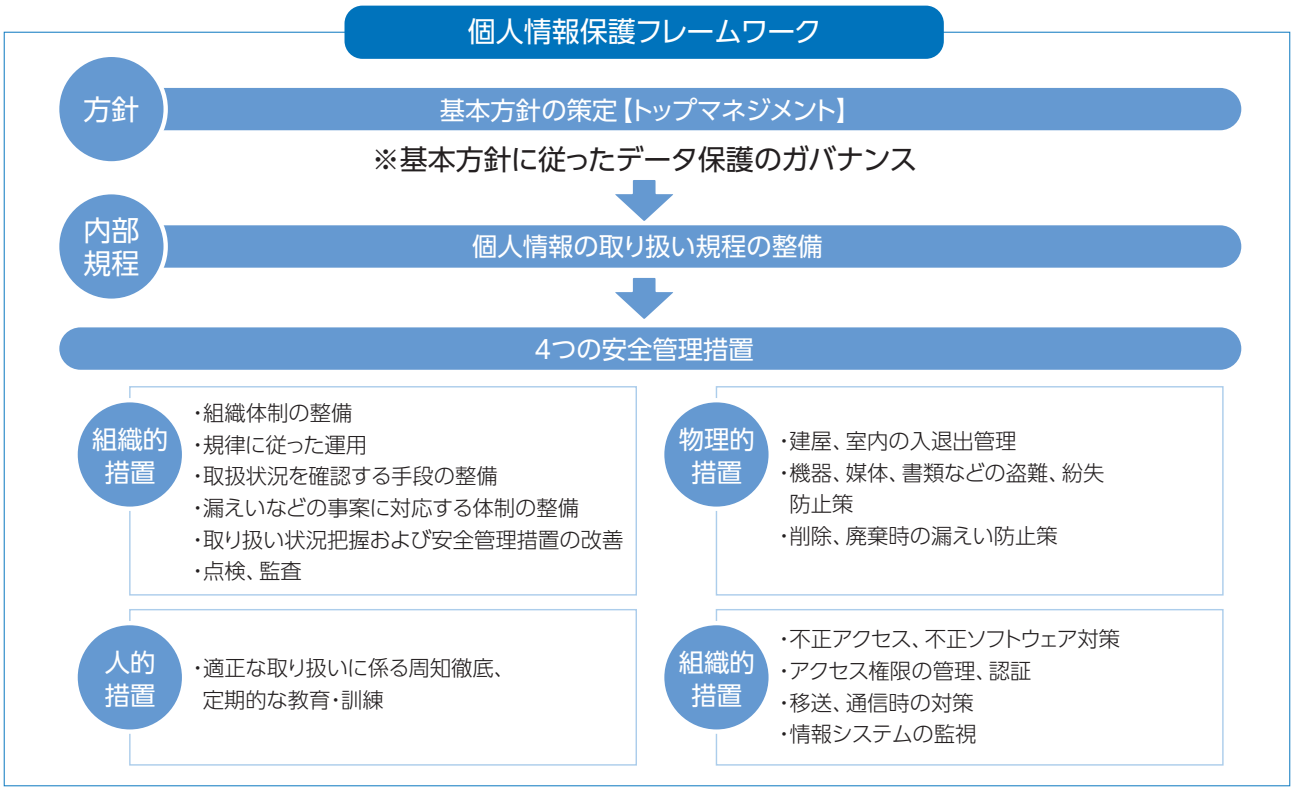
組織的安全管理措置では、個人情報保護責任者を設置し、個人情報保護体制を整備しています。（「個人情報保護体制」を参照）

個人情報の安全管理に関する従業者の役割・責任や個人情報の取り扱いに関する規定などを定め、それに従った運用を実施しています。また、漏えい事故などの発生時の対応体制の整備や点検監査に係る規定を定め、運用を実施しています。

人的安全管理措置では、個人情報保護の教育計画に基づき、階層別教育、専門教育、全従業員eラーニングなど、個人情報の適正な取り扱いに係る各種教育、訓練を実施しています。（「個人情報保護に関する教育」を参照）

物理的安全管理措置では、各所建屋や室内の入退管理や機器・書類などの物理的な保護、盗難などに対する対策、また、機器・書類などの廃棄時の漏えい防止策といった安全対策を行っています。

技術的安全管理措置では、情報システムに対する不正アクセス、不正ソフトウェア対策の実施などを行っています。また、取り扱う個人情報の重要度に応じてアクセス権限の管理、認証、移送、通信時の対策、情報システムの監視などを行っています。



個人情報の管理と適切な取り扱い

日立では、個人情報保護法より一段高いレベルの管理を行うためにJIS規格「個人情報保護マネジメントシステム−要求事項」（JIS Q 15001）相当の社内規程を制定し、規則にのっとり、厳格な管理と適切な取り扱いに努めています。職場ごとに個人情報管理の責任者（情報資産管理者）を置き、業務で取り扱う「すべての個人情報」を特定し、当該個人情報の重要性およびリスクに応じて、台帳を管理し、適切な措置を講じています。

個人情報の取り扱い業務ごとにリスクの認識、分析を実施し、取り扱いに関するルールを定めて運用する「個人情報取扱業務」は、全社一括管理を行っており、定期的に見直しを実施しています。

また、個人情報取扱者には、当該業務の取り扱いルールの周知徹底を行い、署名をしてから業務を開始しています。運用時は、1か月に1回職場での自主点検を行い、安全管理措置や運用状況を定期的に確認しています。

マイナンバー制度への対応

日立では、マイナンバー制度に対応した社内規程にのっとり、厳格な管理と適切な取り扱いに努めています。マイナンバーの管理体制を確立して、マイナンバー取り扱い業務のリスクを評価し、適切な措置を講じています。

個人情報保護に関する監査

日立製作所および国内すべてのグループ会社で1年に1回個人情報保護および情報セキュリティの監査を実施しています。

日立製作所における監査は、執行役社長から任命された監査責任者が独立した立場で実施、監査の公平性・独立性を確保するため、相互監査を行っています。

日立製作所を含む国内の全グループ会社（196社）については、日立製作所と同等の監査を実施し、その結果を日立製作所が確認しています。

情報セキュリティ監査では、個人情報保護、管理の順守事項を確認し、法令への適合性を監査します。

個人情報保護に関する教育

個人情報の確実な保護のため日立ではすべての役員、従業員、派遣社員などを対象にeラーニングによる教育を毎年実施しています。

詳細は「情報セキュリティマネジメント」の「情報セキュリティに関する教育」をご参照ください。

委託先の管理強化

日立では、早くから個人情報の委託先管理を強化し、個人情報の取り扱いを委託する際の社内規程を定め、委託先の審査や監督を実施しています。業務を委託する際には、日立と同等以上の個人情報保護の水準にある委託先を選定するために、委託先審査を行っています。さらに、管理体制の確立、再委託原則禁止など厳格な個人情報管理条項を盛り込んだ契約を締結したうえで、委託しています。また、定期的に委託先の審査を実施し委託先に責任の自覚を促すなどを行い、委託先の管理・監督を推進しています。

グローバルでの個人情報保護の取り組み

デジタル化の著しい進展を受けてデータの利活用が進んでいる昨今、プライバシーリスクも増大しており、個人情報保護への要請も高まっています。この状況下、世界各国で個人情報保護関連法制度の制定・改定の動きが活発になっています。

国境をまたいでデータの利活用がなされることもあり、各国法制度では保護対象となる個人情報が自国内のものに限定されなかったり、他国への越境移転を規制していたりする場合があります。このため、個人情報保護のコンプライアンス対応では各国法制度の動向を把握した上で適切な対応を進める必要があります。

日立では、グローバルでの個人情報保護法制対応の先駆けとして、欧州一般データ保護規則（GDPR）への対応推進を図ってまいりました。欧州の地域統括会社、欧州事務所を含む日立グループ全体で連携し、GDPRの適用を受ける業務の特定とそのリスク評価、リスクに応じた適切な安全管理措置の実行、全従業員を対象とした教育などを実施しています。

また、そのほかのデータ保護法令に対しても現地の地域統括会社などと連携しながら対応を推進しています。日立グループ内の個人情報保護に関するリスク状況を把握し、適切な対処を進めるため、各社の対応状況を継続してモニタリングし、適切な措置を講じています。

今後も引き続き、海外グループ会社の個人情報保護のコンプライアンス対応を支援するため、各国の対応機能の強化・整備に取り組みます。

コラム

日立グループのプライバシーマーク※への取り組み

日立グループでは、グループ一体となり、個人情報保護に取り組んでいます。1998年にグループ会社が初取得して以来、2020年8月末日現在、39事業者が「プライバシーマーク」を取得し、法令より管理レベルの高い個人情報の保護と取り扱いを行っています。

日立製作所は、2019年3月、7回目の更新を取得し、2021年3月に向け8回目の更新に取り組んでいます。

また、プライバシーマーク取得会社を主体として、「日立グループPマーク連絡会」を組織し、定期的に情報交換会、勉強会、外部有識者を招いての講演会などを実施するほか、グループ全体として、個人情報保護に関する情報共有および研鑽（けんさん）を重ねています。

一般財団法人日本情報経済社会推進協会 プライバシーマーク制度のWebサイトへ（https://privacymark.jp/）

※ プライバシーマークとは：適切に個人情報の安全管理・保護措置を講じていると認められた事業者に付与される、第三者認証（付与機関：一般財団法人日本情報経済社会推進協会）

日立グループ プライバシーマーク付与事業者

日立グループのプライバシーマーク付与事業者は、以下のとおりです（2020年8月末日現在）。

株式会社日立製作所
株式会社日立製作所　病院統括本部
日立健康保険組合
沖縄日立ネットワークシステムズ株式会社
株式会社九州日立システムズ
株式会社四国日立システムズ
株式会社セキュアブレイン
株式会社日立ICTビジネスサービス
日立SC株式会社
株式会社日立アーバンサポート
株式会社日立アカデミー
株式会社日立インフォメーションエンジニアリング
日立オムロンターミナルソリューションズ株式会社
株式会社日立ケーイーシステムズ
株式会社日立コンサルティング
株式会社日立産業制御ソリューションズ
株式会社日立システムズ
株式会社日立システムズエンジニアリングサービス
株式会社日立システムズネットワークス
株式会社日立システムズパワーサービス
株式会社日立システムズフィールドサービス
株式会社日立社会情報サービス
株式会社日立情報通信エンジニアリング
株式会社日立総合計画研究所
株式会社日立ソリューションズ
株式会社日立ソリューションズ・クリエイト
株式会社日立ソリューションズ西日本
株式会社日立ソリューションズ東日本
株式会社日立ドキュメントソリューションズ
株式会社日立ハイシステム21
株式会社日立ハイテクソリューションズ
株式会社日立パワーソリューションズ
株式会社日立ビルシステム
株式会社日立フーズ&ロジスティクスシステムズ
日立ヘルスケアシステムズ株式会社
株式会社日立保険サービス
株式会社日立マネジメントパートナー
株式会社日立リアルエステートパートナーズ
株式会社北海道日立システムズ

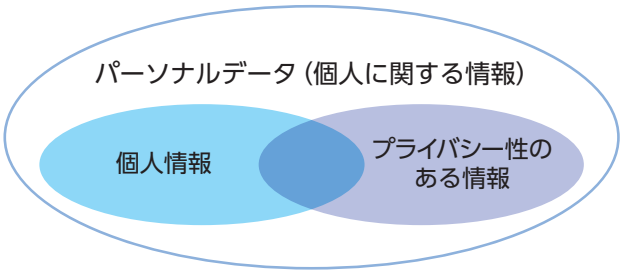
プライバシー保護の取り組み

IoTやAI、ロボティクスなどの技術進展に伴い、多種多量なデータの利活用による社会イノベーションの実現が期待される一方で生活者のプライバシー保護への関心も高い状況にあります。日立は、安全・安心を確保した価値創出に向けてプライバシー保護に取り組んでいます。

パーソナルデータの利活用とプライバシー保護

昨今、個人情報に該当するかどうかを問わず、個人に関する情報がパーソナルデータと総称され、その利活用による価値創出が期待される一方で個人のプライバシーへの配慮が求められています。加えて、IoT時代においては、収集されるパーソナルデータがますます増え、プライバシーにかかわるリスクも変化しています。

右図に示す通り、パーソナルデータには、個人情報と一部重複して、「位置情報」や「購買履歴」などのプライバシー性のある情報が含まれます。パーソナルデータを利活用した価値創出のためには、個人情報を保護するとともに、プライバシーを保護していく必要があります。



日立のプライバシー保護の取り組み

日立は、パーソナルデータの安全・安心な利活用による価値創出をめざし、ITセクターが中心となって2014年からデータ利活用におけるプライバシー保護に取り組んでいます。

●プライバシー保護諮問委員会の運営

日立は、デジタル事業をけん引するITセクターにおいてパーソナルデータの取り扱いを統括する「パーソナルデータ責任者」と、プライバシー保護に関する知見を集約してリスク評価や対応策検討を支援する「プライバシー保護諮問委員会」を設置しています。

●プライバシー保護に関する規則・マニュアルの整備

日立では、このような体制のもとでプライバシー保護方針を定め、方針に沿ってパーソナルデータの取り扱い規則を制定し、従業員向けのマニュアルを整備しています。マニュアルでは、プライバシー保護のための具体的なプロセス、留意事項などを解説することで、個々の従業員がプライバシー保護対策を実践できるようにしています。

●プライバシー影響評価の実施

このような規則・マニュアルに従って、従業員はパーソナルデータを取り扱う業務においてプライバシー影響評価を実施し、プライバシーにかかわる問題の発生を防ぐための対策を講じています。評価にあたっては法制度や技術の動向、問題化事例、後述する意識調査から得られた知見などから日立が独自に作成したチェックリストを使用します。このとき、従業員だけでは判断が難しい場合や、リスクが高いと評価された場合には、プライバシー保護諮問委員会が対応を支援し、リスクの低減を図っています。

日立は、これまで多くの業務にプライバシー影響評価を適用しており、その件数は2019年度だけで190件に及びます。対象となった業務分野も金融、公共、社会インフラ、産業・流通など、多岐にわたっています。

●プライバシー保護教育

パーソナルデータ利活用とプライバシー保護の両立を図るためには、個々の社員がその重要性を理解し、プライバシー対策を実践する必要があります。そのため、プライバシー保護に関する定期的な教育や情報共有を行うとともに、プライバシー保護のあり方について検討しています。

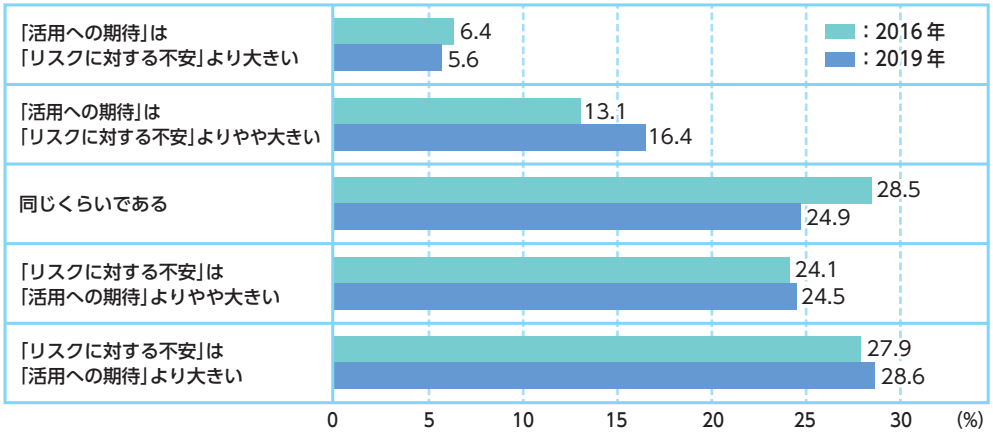
生活者およびお客さまの安全・安心をめざして

日立は、プライバシー保護に関する生活者の期待に対応するため、2019年に株式会社 博報堂とともに「第四回 ビッグデータで取り扱う生活者情報に関する意識調査」を実施しました※。パーソナルデータの利活用について「不安が期待より大きい」という回答が前回調査から微増し、引き続き過半数を占めました。また、生活者の中にもプライバシー保護に関し「企業などによる対策を期待する層」と「自衛傾向が強い層」という異なる意識を持つ2つのグループが存在することが明らかになりました。人々の意識が多様化し、きめ細やかなプライバシー対策の必要性が浮き彫りになっており、これら生活者の意識の変化をプライバシー保護対策に反映しています。

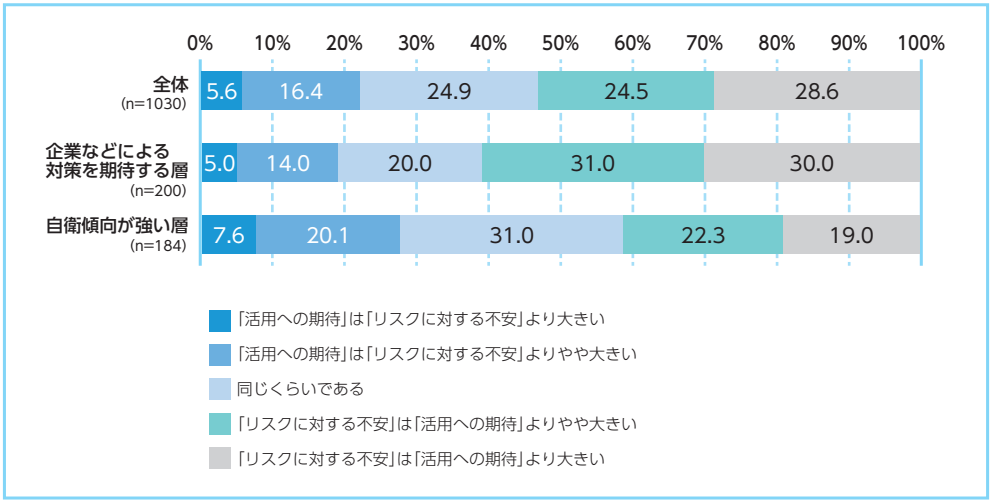
日立は、これまで多数の業務でプライバシー保護に対応したノウハウをお客さまとのビジネスにおいても活用し、プライバシーに配慮したより良いサービスや技術をお客さまに提供していくことで安全・安心な社会イノベーションの実現に貢献していきます。

※「第四回 ビッグデータで取り扱う生活者情報に関する意識調査」(2019年6月公表)
https://www.hitachi.co.jp/New/cnews/month/2019/06/0606.html

Q 企業や公的機関などによるパーソナルデータの活用に関して、どのように感じますか。「活用への期待」と「リスクに対する不安」のどちらが大きいかをお答えください。



Q 企業や公的機関などによるパーソナルデータの活用に関して、どのように感じますか。「活用への期待」と「リスクに対する不安」のどちらが大きいかをお答えください。



組織を越えたセキュリティ連携技術の研究開発

サイバー攻撃の巧妙化により、単一組織での対策は限界を迎えつつあります。このような問題に対処するため、組織を越えたセキュリティ連携技術の研究開発に取り組んでいます。

はじめに

サイバー攻撃のスピードは年々高まっており、短時間に多拠点が攻撃されるリスクは増加しています。さらに、クラウドやBYOD (Bring Your Own Device) の進展で守るべき対象が自組織のシステムからクラウドや個人端末にまで拡大しており、革新的なセキュリティ対策が求められています。

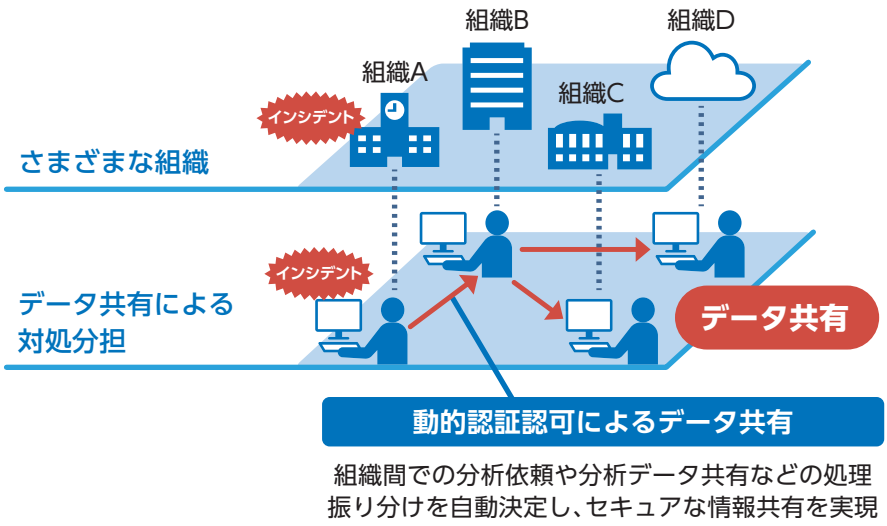
これに対し、日立は、慶應義塾大学、中部電力株式会社と共に、お互いが持つセキュリティ情報を共有し、連携して対処する「分散型セキュリティオペレーション」の研究開発に取り組んでいます。

分散型セキュリティオペレーション構想

従来のインシデントレスポンスでは、特定のセキュリティ対応チームをハブとして、インシデント情報と分析データ (ログ、不審データ、通信パケット) を集約し、人手作業で複数のセキュリティ対応チームに分析依頼と分析データの送付を行っていました。今回策定した「分散型セキュリティオペレーション」構想では、特定のセキュリティ対応チームがすべてのインシデントレスポンスに関与するのではなく、クラウドプロバイダなどの各組織にあるセキュリティ対応チームが自律分散的にインシデントに対処し、必要に応じて連携します。

「分散型セキュリティオペレーション」の中核技術の一つとなる「動的認証認可技術」では、情報収集や分析などのインシデントレスポンスに求められる機能を標準化して、それぞれのセキュリティ対応チームが持つ機能を互いにリアルタイムで確認できるようにしました。これにより、分析依頼や分析データ共有などの処理をどの専門チームへ委託するかを機械的に振り分けること (認可) を可能にします。さらに、関与する組織が新た判明する度に、認可からデータ送受信組織の承認 (認可) までの一連の処理を自動的に行うことで、迅速なセキュリティ対策を実現します。

本技術の効果を検証するため、慶應義塾インフォメー



ションテクノロジーセンターで監視しているインシデントの分析対象データを、日立オープンラボ横浜にある研究用のSOCに送付し、分析を委託する実証環境を構築して評価しました。この結果、従来は担当者の習熟度によって、数分から数時間とばらつきのあった「インシデント検知から分析を依頼する一連の処理」を1秒以内に完了できることを確認しました。

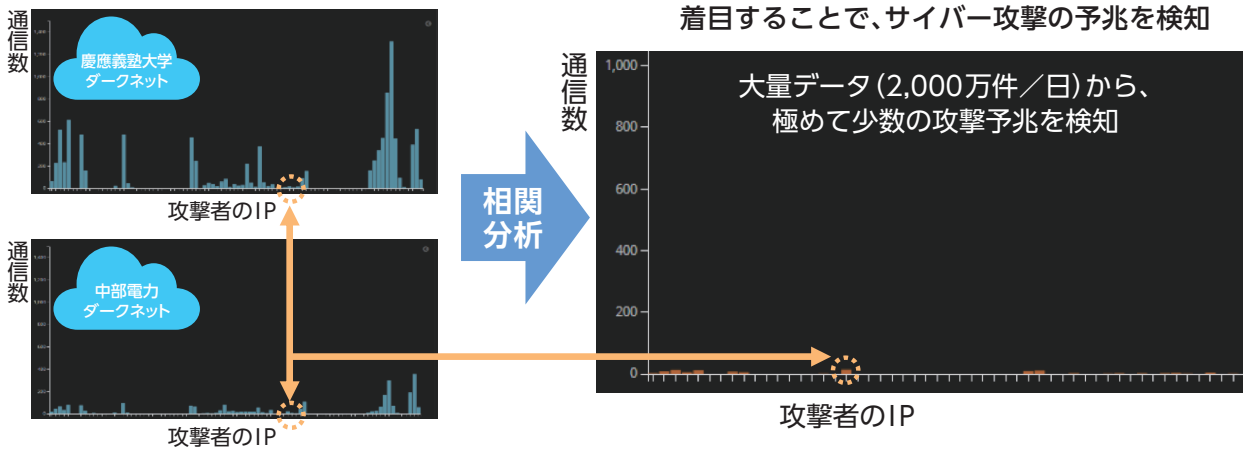
サイバー攻撃の予兆検知

「分散型セキュリティオペレーション」構想のもと、複数組織のダークネット通信情報を共有・分析することにより、サイバー攻撃の予兆を検知できることを実証しました。

従来、サイバー攻撃の予兆検知には、通常業務では使われないIPアドレスとの通信であるダークネット通信の監視が用いられてきました。しかし、目立たない攻撃の検知は難しく、また攻撃であると断定するまでに数か月を要するという課題がありました。このような問題に対し、日立と慶應義塾大学は、攻撃者が短期間に複数の組織を攻撃可能か下見する特性に着目し、複数組織のダークネット通信に紛れる不審通信を相関分析する技術を開発しました。さらに、攻撃につながる連続した通信の増加のみを機械学習で抽出するトラフィック遷移モデルを開発し、攻撃の早期予兆検知を実現しました。

これらの技術を用い、日立オープンラボ横浜にて慶應義塾大学と中部電力で観測した大量のダークネット通信（2,000万件/日）を分析し、このうち極めて少数の通信でもサイバー攻撃の予兆として検知できること、公的機関から注意喚起される平均45日前（最長81日前）に予兆検知できることを確認しました。

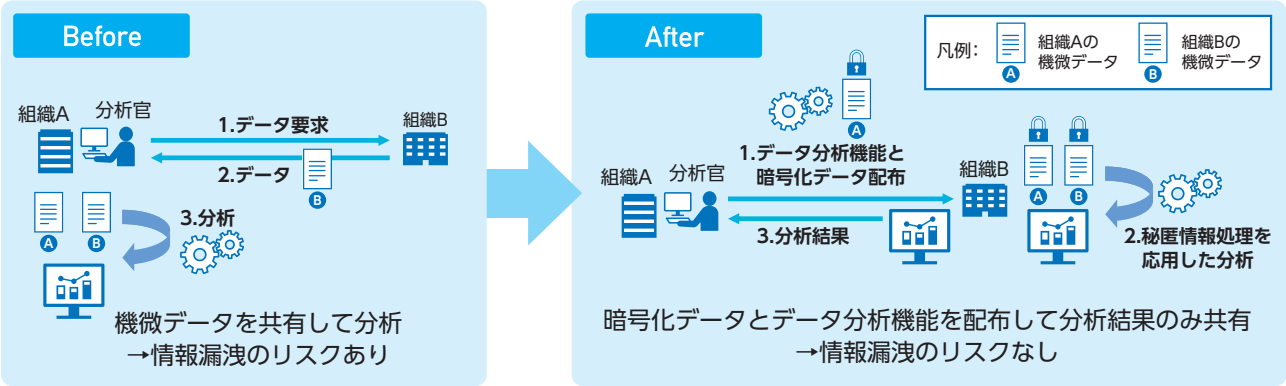
複数組織に共通して現れる少数の不審通信に着目することで、サイバー攻撃の予兆を検知



機微データの組織間共有

「分散型セキュリティオペレーション」では、セキュリティ情報を複数組織で共有することで迅速な対処を実現します。一方で、機微なデータの開示にはリスクがあるため、共有を躊躇(ちゅうちょ)するということも考えられます。このような問題に対し、機微データを開示することなく分析結果だけを共有するVDS (Verifiable Decentralized Secrets analysis) 技術の開発を進めています。

セキュリティ情報の共有では、必ずしも生データ自体を必要としているわけではありません。例えば、自組織と同じ攻撃を受信した組織を発見することや、コミュニティ内で同じ攻撃を受けた組織数を調査する場合には、攻撃に関するメールやログといった生データ自体は必要ではなく、共通の情報を持っているかどうかという情報のみが必要とされます。そこで、機微データを開示することなく分析結果だけを共有するVDSシステムを開発中です。本システムでは、データ自体は共有せずに、データを分析する機能を配布・実行し、データ分析のために必要十分な情報のみを共有します。これにより、機微データの開示を抑えることができ、情報共有を促進することが期待できます。



VDSを活用した分析の事例として、不審メールの情報共有による、攻撃の目的・規模推定が挙げられます。社会インフラ系組織である組織Aは、受信した不審メールと類似したメールを受信したかどうかを、学術系組織である組織Bと、社会インフラ系組織Cに問い合わせます。

組織B、組織Cは、組織Aの問い合わせ内容を知ることなく、また、自組織のメール内容を開示することなく、類似メールの有無を組織Aに返答します。組織Aは、組織Bには類似メールが届いておらず、組織Cには類似メールが届いているという事実から、攻撃者は社会インフラ系を対象として攻撃を行っていると推定することができます。

現在、本技術の有効性を検証するための実証実験に取り組んでいます。


Check the reception status at other organizations

問合せ結果

	○○電力	□□電力	△△電力	●●電力	■■電力	▲▲自動車	▽▽自動車
受信有無	✓	✓	✓	✓	✓	×	×
判断結果	悪性	悪性	悪性	判定中	悪性	-	-
判断根拠	ABC Anti-virus	Sender-blacklisted	オペレータ分析結果	-	URL-suspicious	-	-

	▼▼自動車	XX自動車	YY製作所	ZZ電機	WW電機	VV電工	◎◎大学
受信有無	×	×	×	×	×	×	×
判断結果	-	-	-	-	-	-	-
判断根拠	-	-	-	-	-	-	-

受信総数	悪性判断数	悪性確率推定結果
5/14	4/5	90.5%

OK

情報セキュリティに関する社外活動

日立では、従業員それぞれの持つ経験や知識を生かし、情報セキュリティに関する各種社外活動に参画することにより、よりセキュアなIT社会の実現のために活動しています。

国際標準化活動

次のセキュリティに関する国際標準化活動に参画しています。

●ISO/IEC JTC1/SC27

国際標準化機構（ISO）と国際電気標準会議（IEC）による国際標準化のための合同技術委員会ISO/IEC JTC1のサブコミッティであるSC27では、情報セキュリティマネジメントシステム（WG1）、暗号とセキュリティメカニズム（WG2）、セキュリティ評価技術（WG3）、セキュリティコントロールとサービス（WG4）、アイデンティティ管理とプライバシー技術（WG5）に関する規格化が検討されています。

●ISO TC292

ISOのテクニカルコミッティ（TC）292では、一般的なセキュリティマネジメント、事業継続マネジメント、レジリエンスおよびエマージェンシーマネジメント、不正防止対策および管理、セキュリティサービス、ホームランドセキュリティなど、さまざまなセキュリティに関する規格化が検討されています。

●ISO TC262

ISOのTC 262はリスクマネジメントをテーマとしており、すべてのリスクを対象とし、用語、原則および指針、リスクアセスメント技法などの規格化が検討されています。

●ITU-T SG17

国際電気通信連合（ITU）の電気通信標準化部門（ITU-T）のスタディグループ（SG）のひとつであるSG17では、サイバーセキュリティ、通信事業者向けセキュリティ管理、テレバイオメトリクス、通信・アプリケーションサービスに対するセキュリティ機能、スパム対策、ID管理などの規格化が検討されています。

●IEC TC65/WG10, WG20

IECのTC 65では産業用オートメーション、計測、制御の標準化が進められています。その中のWG10では、制御システムにおけるネットワークと制御装置のセキュリティに関する規格化が検討されています。また、WG20では、制御システムにおけるセキュリティと機能安全の両立に関する規格化が検討されています。

●OASIS CTI

構造化情報標準促進協会（OASIS）のサイバー脅威インテリジェンス（CTI）では、サイバー攻撃活動を記述し、交換するための脅威情報構造化記述形式、検知指標情報自動交換手順に関する規格化が検討されています。

シーサート（CSIRT）活動

日立では、日立グループにおけるシーサート活動に加え、HIRT（Hitachi Incident Response Team）を窓口（PoC:Point of Contact）として社外シーサート活動に参画しています。また、社外シーサート組織などとの連携として、脆弱性などに関する情報の共有・交換を推進しています。

●FIRST

FIRST（Forum of Incident Response and Security Teams）は、大学、研究機関、企業、政府機関などが加盟する信頼関係に結ばれたインシデント対応チームの国際コミュニティです。2020年7月末時点で、96か国、539チームが加盟しています。

●日本シーサート協議会（NCA）

日本で活動するシーサート組織間の情報共有・連携を通して、シーサート活動上の課題解決を図るために設立された団体です。シーサート設立の促進・支援、インシデント発生した場合のシーサート間の連携体制作りなど、国内のシーサートコミュニティが、いざというときに協力できるよう、組織自身が自主的に「インシデント対応基礎能力」の向上を図れる場を提供しています。日立は、協議会発足メンバーであり、2015年からは運営委員長の立場で、国内のシーサート活動の普及を推進しています。

そのほかの活動

上記活動に加えて、次に示すセキュリティに関する研究・検討、普及・啓発などを推進する各種社外活動へ参画しています。また、全国で開催される各種セミナー、学会などにおける講演も行っています。

- 独立行政法人情報処理推進機構（IPA）10大脅威執筆者会 ほか
- 一般財団法人日本情報経済社会推進協会（JIPDEC）ISMS専門部会、制御システムSMS専門部会 ほか
- 一般財団法人日本サイバー犯罪対策センター（JC3）
- 特定非営利活動法人日本セキュリティ監査協会（JASA）
- NPO日本ネットワークセキュリティ協会（JNSA）
- 日本セキュリティオペレーション事業者協議会（ISOG-J）
- 日本ISMSユーザグループ（J-ISMS UG）
- 一般社団法人日本電気計測器工業会（JEMIMA）PA・FA計測制御委員会、セキュリティ調査研究WG
- 技術研究組合制御システムセキュリティセンター（CSSC）
- 一般社団法人電子情報技術産業協会（JEITA）情報セキュリティ調査専門委員会 ほか
- 一般社団法人ICT-ISAC
- フィッシング対策協議会
- 独立行政法人製品評価技術基盤機構（NITE）評価機関認定技術委員会
- ロボット革命イニシアティブ協議会 産業セキュリティアクショングループ
- 一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ検討会、セキュリティ品質検討委員会 ほか

第三者評価・認証

日立では、情報セキュリティマネジメントに関する第三者評価・認証の取得を推進しています。

ISMS認証取得状況

日立が、一般社団情報マネジメントシステム認定センター（ISMS-AC）から情報セキュリティマネジメントシステム国際規格（ISO/IEC 27001）に基づくISMS認証を取得した組織は、以下のとおりです（2020年8月末日現在）。なお、以下の組織名はISMS-ACによるISMS認証取得組織一覧の表記を用いています。

- 株式会社日立製作所（金融第二システム事業部 公共系金融システム部門）
- 株式会社日立製作所（サービス&プラットフォームビジネスユニット制御プラットフォーム統括本部）
- 株式会社日立製作所（サービスプラットフォーム事業本部）
- 株式会社日立製作所（水・環境ビジネスユニット　水事業部 ソリューション事業推進部、水・環境ビジネスユニット　環境事業部　情報システムエンジニアリング部、インダストリー事業統括本部　IT・業革推進本部　情報保全センタ）
- 株式会社日立製作所（社会システム事業部グローバルデジタル推進センタ、企画本部、エネルギーシステム第一本部、エネルギーシステム第二本部、エネルギーソリューション本部 および交通情報システム本部）
- 株式会社日立製作所（社会ビジネスユニット　公共システム事業部）
- 株式会社日立製作所 ディフェンスビジネスユニット（横浜事業/池袋分室）および株式会社日立アドバンストシステムズ（本社）
- 株式会社九州日立システムズ（アプリケーション事業部）
- 株式会社四国日立システムズ
- 日本スペースイメージング株式会社
- 株式会社日立ICTビジネスサービス（プロダクトサポート部 メディアサービスグループ）
- 株式会社日立医薬情報ソリューションズ（東京本社）
- 株式会社日立医薬情報ソリューションズ（大阪本社）
- 株式会社日立インフォメーションエンジニアリング
- 日立SC株式会社（本社）
- 日立オムロンターミナルソリューションズ株式会社
- 株式会社日立ケーイーシステムズ（東京オフィス開発センター）
- 株式会社日立システムズ（金融プラットフォーム事業部ソリューション本部　クラウド基盤サービス部）
- 株式会社日立システムズ（公共・社会事業グループ）
- 株式会社日立システムズ（公共・社会プラットフォーム事業部）
- 株式会社日立システムズ（コンタクトセンタ&ビジネスサービス事業部）
- 株式会社日立システムズ（SHIELD　セキュリティセンタ）
- 株式会社日立システムズ（スマートソーシング&サービス事業部）
- 株式会社日立システムズパワーサービス（マネージドサービス事業部　プラットフォームサービス本部　プラットフォームサービス部）
- 株式会社日立システムズフィールドサービス（支社統括本部 首都圏支社　首都圏支店）
- 株式会社日立社会情報サービス（本社、東京本社、阿佐ヶ谷事業所、大森本田ビル）および沖縄日立ネットワークシステムズ株式会社（本社、嘉手納開発センター）
- 株式会社日立ソリューションズ・クリエイト
- 株式会社日立ソリューションズ西日本（クラウド基盤運用サポート部、金融第1ソリューション本部 第5部）
- 株式会社日立ソリューションズ
- 株式会社日立ハイテクソリューションズ（ソリューションセンター）
- 株式会社日立パワーソリューションズ
- 株式会社日立フーズ&ロジスティクスシステムズ
- 株式会社日立マネジメントパートナー
- 株式会社北海道日立システムズ（公共・社会事業統括本部企業サービス事業統括本部　事業企画部　営業本部　産業・流通営業部　金融営業部　地域営業部　IPT営業グループ　システム事業本部　プラットフォーム事業本部　道央サービス推進部　ファシリティ事業推進部　デジタル事業推進部　IPT事業推進部　経営戦略推進本部生産技術管理本部）

ITセキュリティ評価・認証の取得状況

(独) 情報処理推進機構 (IPA) が運用するISO/IEC 15408に基づく「ITセキュリティ評価および認証制度」によって認証された主な製品は、次のとおりです (2020年6月末現在[認証製品アーカイブリストへの掲載を含みます])。

製　品	TOE種別※1	認証番号	評価保証レベル※2
HiRDB/Parallel Server Version 8 08-04	データベース管理システム	C0225	EAL4+ALC_FLR.1
HiRDB/Single Server Version 8 08-04	データベース管理システム	C0216	EAL4+ALC_FLR.1
HiRDB Server Version 9 (Linux版) 09-01	データベース管理システム	C0351	EAL2+ALC_FLR.2
Smart Folder PKI MULTOS application 03-06	スマートカード用アプリケーションソフトウェア	C0014	EAL4
Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software 8.0.1-02	Access Control Device and Systems	C0536	EAL2+ALC_FLR.1
Hitachi Virtual Storage Platform G1000, Hitachi Virtual Storage Platform VX7 Control Program 80-01-25-00/00 (R8-01A-06_Z)	ストレージ装置制御ソフトウェア	C0514	EAL2+ALC_FLR.1
Hitachi Unified Storage VM Control Program 73-03-09-00/00 (H7-03-10_Z)	ストレージ装置制御ソフトウェア	C0513	EAL2+ALC_FLR.1
Hitachi Unified Storage 110用マイクロプログラム　0917/A	ストレージ装置制御ソフトウェア	C0421	EAL2
Hitachi Unified Storage 130用マイクロプログラム　0917/A	ストレージ装置制御ソフトウェア	C0420	EAL2
Finger Vein Authentication Device UBReader2 Hardware: D, Software: 03-00	生体認証装置	C0332	EAL2
証明書検証サーバ 03-00	PKI	C0135	EAL2
CBTエンジン 01-00	CBT試験システム 主要アプリケーション	C0288	EAL1+ASE_OBJ.2、 ASE_REQ.2、ASE_SPD.1
汚染拡大防止システム SHIELD/ExLink-IA 1.0	セキュリティ管理ソフトウェア	C0090	EAL1

※1 TOE (Target Of Evaluation)
評価の対象となるソフトウェアやハードウェアなどの製品のことをTOEといいます。関連する管理者および使用者の手引書 (利用者マニュアル、ガイダンス、インストール手順書など) を含むことがあります。

※2 EAL (Evaluation Assurance Level)
ISO/IEC 15408では、規定した評価項目 (保証要件) に対する保証の度合いを、EAL1から7まで7段階のレベルで規定しており、段階が上がるごとに評価の内容が厳しくなります。
・EAL1は、セキュリティ機能の妥当性とテスト、セキュリティを維持するためのガイダンスが客観的に評価されます。
・EAL2は、一般的な攻撃能力を想定した脆弱性分析、製造から運用開始まで、製品の完全性の観点から評価が追加されます。通常の開発ライフサイクルにセキュリティ的な視点を加味しています。
・EAL3は、EAL2で得られる保証に加えて、テストの網羅性や開発時の製品の改ざんを防止するための開発環境の評価が実施されます。
・EAL4は、一般的な商用製品として最高位とされており、開発環境での開発資産の保全性やソースコード、要員の信頼性など開発ライフサイクル全般にわたって評価されます。
・ALC_FLR.1は、製品にセキュリティの欠陥が発見された場合、必要なパッチを提供する基本的な手続きを客観的に評価します。規格では規定のEALに含まれない保証要件を追加することができ、その場合、EAL2+ALC_FLR.1のように表記します。
ALC_FLR.2は、利用者からの脆弱性情報の報告受け付けと利用者への通知手続きが求められます。

暗号モジュール試験・認証の取得状況

IPAが運用するISO/IEC 19790に基づく「暗号モジュール試験および認証制度（JCMVP）」または米国NISTとカナダCSEが運用するFIPS140-2に基づく「Cryptographic Module Validation Program（CMVP）によって認証された主な製品は、次のとおりです（2020年6月末現在）。

製　品	認証番号	レベル
Hitachi Flash Module Drive HDE	3314	Level 2
Hitachi Virtual Storage Platform（VSP）Encryption Board	3279	Level 1
Hitachi Virtual Storage Platform（VSP）Encryption Module	3278	Level 2
Hitachi Virtual Storage Platform（VSP）Encryption Adapter	2727	Level 2
Hitachi Virtual Storage Platform（VSP）Encryption Board	2694	Level 1
Hitachi Virtual Storage Platform（VSP）Encryption Module	2462	Level 2
Hitachi Virtual Storage Platform（VSP）Encryption Engine	2386	Level 1
Hitachi Unified Storage Encryption Module	2232	Level 1
HIBUN Cryptographic Module for User-Mode 1.0 Rev.2	JCMVP #J0015、CMVP#1696	Level 1
HIBUN Cryptographic Module for Kernel-Mode 1.0 Rev.2	JCMVP #J0016、CMVP#1697	Level 1
HIBUN Cryptographic Module for Pre-boot 1.0 Rev.2	JCMVP #J0017、CMVP#1698	Level 1
Keymate/Crypto JCMVP ライブラリ（Solaris版 および Windows版）	JCMVP #J0007	Level 1
Keymate/Crypto JCMVPライブラリ	JCMVP #J0005	Level 1

日立グループの概要

会社概要 (2020年3月31日現在)

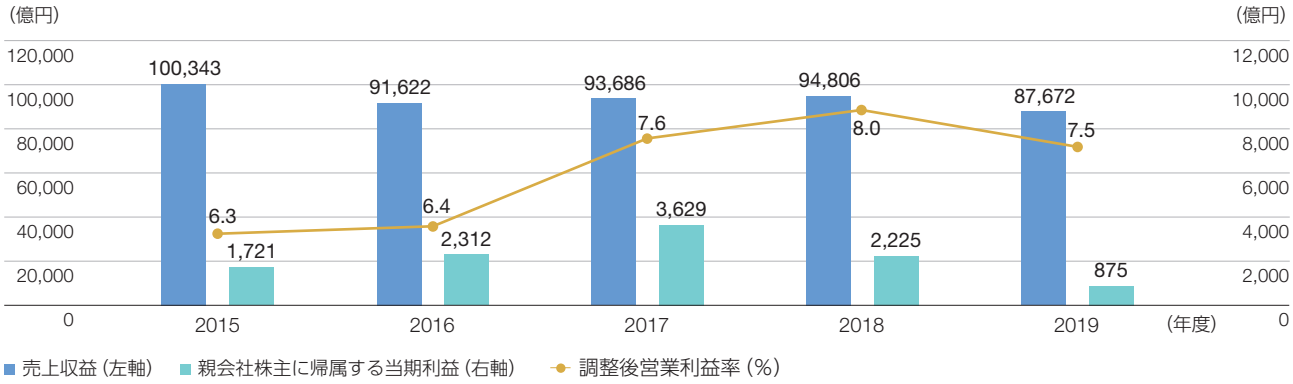
商号	株式会社日立製作所
設立年月日	大正9年 (1920年) 2月1日 (創業明治43年〈1910年〉)
本店の所在地	東京都千代田区丸の内一丁目6番6号
代表者	執行役社長兼CEO 東原敏昭
資本金	458,790百万円
従業員数 (個別)	3万1,442人
(連結)	30万1,056人
連結子会社数	814社 (国内173社、海外641社)
持分法適用会社数	409社

財務ハイライト (2020年3月期連結IFRS)

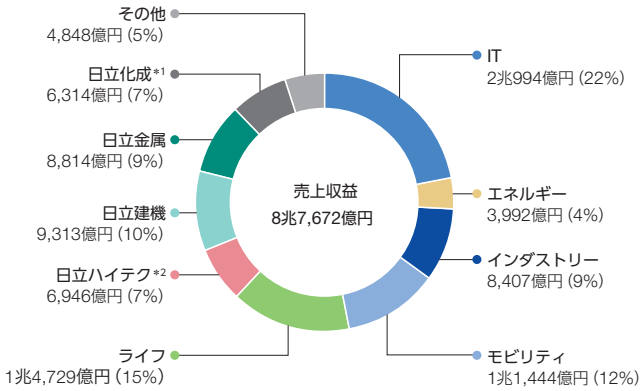
売上収益	8兆7,672億円 (前期比92%)
調整後営業利益率	7.5% (前期比0.5ポイント減)
EBIT*1	1,836億円 (前期比36%)
当期利益 (親会社株主帰属)	875億円 (前期比39%)
ROIC*2	9.4% (前期比0.9ポイント増)
設備投資額	3,996億円 (前期比96%)
研究開発費	2,937億円 (前期比91%)

※ 当社の連結財務諸表は、国際財務報告基準 (IFRS) に基づいて作成しています
*1 EBIT:継続事業税引前当期利益から、受取利息の額を減算し、支払利息の額を加算して算出した指標
*2 ROIC:Return on invested capitalの略で「投資資本利益率」の意。「ROIC=(税引後の調整後営業利益率+持分法損益) ÷投下資本×100」により算出。
なお、税引後の調整後営業利益=調整後営業利益×(1−税引負担率)、投下資本=有利子負債+資本の部合計

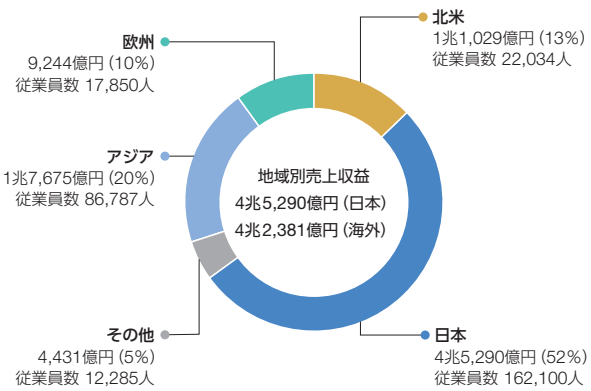
●売上収益／調整後営業利益率／当期利益の推移



●セグメント別売上収益／構成比 (2020年3月期 連結IFRS)



●地域別売上収益／構成比 (2020年3月期 連結IFRS)



※各部門の売上収益は、部門間内部売上収益を含んでいます
*1 2020年4月株式売却済
*2 2020年5月完全子会社化

株式会社 日立製作所
情報セキュリティリスク統括本部
〒100-8280 東京都千代田区丸の内一丁目6番6号
TEL.03-3258-1111

Printed in Japan (H) (2020.12)